AudioCodes™ CPE & Access Analog Gateways

SIP

MediaPack™ MP-124 & MP-11x

Release Notes Version 5.0

Document #: LTRT-65608

December 2006

Table of Contents

1 What's New in Release 5.0 7

1.1 Supported Hardware Platforms 7
1.1.1 New Hardware Platforms Introduced in this Release 7
1.1.2 Support for Existing Hardware Platforms 7
1.1.3 Hardware Platforms No Longer Supported 7
1.2 General Gateway New Features 8
1.3 SIP New Features 11
1.4 Web and SNMP New Features 16
1.5 Resolved Constraints 17
1.6 New Parameters 18
1.7 Modified Parameters 25
1.8 Obsolete Parameters 35

2 SIP Compatibility 37

2.1 Supported SIP Features 37
2.2 Unsupported SIP Features 39
2.3 SIP Compliance Tables 40
2.3.1 SIP Functions 40
2.3.2 SIP Methods 40
2.3.3 SIP Headers 40
2.3.4 SDP Headers 42
2.3.5 SIP Responses 42

3 Known Constraints 47

3.1 Hardware Constraints 47
3.2 SIP Constraints 47
3.3 Gateway Constraints 47
3.4 Web Constraints 49
3.5 SNMP Constraints 50

4 Previous Release 4.8 53

4.1 Supported Hardware Platforms 53
4.1.1 New Hardware Platforms Introduced in This Release 53
4.1.2 Existing Hardware Platforms 53
4.1.3 Hardware Platforms No Longer Supported 53
4.2 General Gateway New Features 54
4.3 SIP New Features 56
4.4 Web and SNMP New Features 58
4.5 Resolved Constraints 58
4.6 New and Modified Parameters 59
4.7 Version History 70

List of Tables

Table 1-1: Release 5.0 New *ini* File [Web Browser] Parameters (continues on pages 18 to 24).....18
Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34).....25
Table 1-3: Release 5.0 Obsolete *ini* File [Web] Parameters.....35
Table 2-1: SIP Functions.....40
Table 2-2: SIP Methods.....40
Table 2-3: SIP Headers (continues on pages 40 to 42).....40
Table 2-4: SDP Headers.....42
Table 2-5: 1xx SIP Responses.....43
Table 2-6: 2xx SIP Responses.....43
Table 2-7: 3xx SIP Responses.....43
Table 2-8: 4xx SIP Responses (continues on pages 44 to 45).....44
Table 2-9: 5xx SIP Responses.....45
Table 2-10: 6xx SIP Responses.....46
Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70).....59

Notices

Notice

This document describes the release of the AudioCodes' MediaPack Analog Media Gateway Series (MP-124 24 port, MP-118 8-port, MP-114 4-port, and MP-112 2-port).

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered Technical Support customers at www.audiocodes.com under Support / Product Documentation.

© Copyright 2006 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: Dec-07-2006 Date Printed: Dec-10-2006

Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the ALT and ◄ keys.

Trademarks

AC logo, Ardito, AudioCoded, AudioCodes, AudioCodes logo, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Stretto, TrunkPack, VoicePacketizer and VoIPerfect, are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used, and only Industry standard terms are used throughout this manual. The symbol 0x indicates hexadecimal notation.

Related Documentation

Document #	Manual Name
LTRT-65407	MP-11x & MP-124 SIP User's Manual
LTRT-59803	MP-11x & MP-124 MGCP-H.323-SIP Fast Track Guide

Notes:

- MediaPack refers to the MP-124, MP-118, MP-114, and MP-112 VoIP gateways.
- MP-11x refers to the MP-118, MP-114, and MP-112 VoIP gateways.

1 What's New in Release 5.0

Note: This document uses a one-row table convention to indicate for which products each feature is applicable. The products that don't support the feature are shaded (grayed). In the example below, the feature would be applicable only to MP-114/MP-118.

MP-112	MP-114/MP-118	MP-124	FXS	FXO

1.1 Supported Hardware Platforms

1.1.1 New Hardware Platforms Introduced in this Release

The following hardware platform is introduced in this version:

- MP-114/FXS+FXO with 2 FXS ports and 2 FXO ports. This product also contains a relay that connects the FXS ports to the FXO ports in case of a power failure.

1.1.2 Support for Existing Hardware Platforms

- MediaPack MP-118/FXS+FXO with 4 FXS ports and 4 FXO ports
- MediaPack MP-11x/FXS, 2 to 8 analog FXS interfaces, with enhanced CPU resources:
  - MediaPack MP-118/FXS, 8 analog FXS interfaces
  - MediaPack MP-114/FXS, 4 analog FXS interfaces
  - MediaPack MP-112/FXS, 2 analog FXS interfaces
- MediaPack MP-124/FXS, 24 analog FXS interfaces

1.1.3 Hardware Platforms No Longer Supported

N/A.

1.2 General Gateway New Features

1. **STUN server support for DNS-SRV:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to provide a domain name for the STUN server's address. The STUN client can perform the required SRV query to resolve the domain name to an IP address and port, sort the server list, and use the servers according to the sorted list.

Relevant parameter: STUNServerDomainName.

2. **Separate interfaces for management and control/bearer:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway can now be configured to operate in Dual IP mode by assigning the same IP address to two traffic types.

When operating with multiple IP interfaces, the gateway splits the traffic into three types: Management (OAM), Control, and Media. Each interface has its own IP and subnet address.

The Dual IP mode option allows the gateway to distinguish between only two traffic types, based on IP address. One of the traffic types consists of a combination of two traffic types (Media and Control, OAM and Control, or OAM and Media), while the other is whichever traffic type excluded in this combination. Therefore, in the Dual IP mode, the same IP address is assigned to two traffic types.

3. **Disable LCP Echos and Link disconnection auto-detection support:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to disable the Point-to-Point Protocol over Ethernet (PPPoE) disconnection auto-detection feature.

By default, the PPPoE Client (embedded on the gateway's software), sends Link Configuration Protocol (LCP) Echo packets to the server to check that the PPPoE connection is open. Some Access Concentrators don't reply to these LCP Echo requests, resulting in a disconnection. By disabling the LCP disconnection auto-detection feature, the PPPoE Client doesn't send LCP Echo packets to the server (and does not detect PPPoE disconnections).

Relevant parameter: PPPoELCPEchoEnable.

4. **IPSec AES support:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports Advanced Encryption Standard (AES) for IPSec/IKE tables.

Relevant parameters: IKEPolicyProposalEncryption_X; IPSecPolicyProposalEncryption_X.

5. **NTT DTMF-based DID support:**

MP-112	MP-114/MP-118	MP-124	FXS

The user can now enable the sending of the NTT (Japanese standard) Direct Inward Dialing (DID) as a DTMF stream.

Relevant parameter: NTTDIDSignallingForm.

6. T.38 packet duplication as No-Op packet (for NAT):

MP-112	MP-114/MP-118	MP-124	FXS	FXO

To enable Network Address Translator (NAT) port binding for T.38 streams, the gateway now supports the sending of T.38 redundant packets to the remote side (including during silence periods), per user-defined interval (in seconds).

Relevant parameters: NoOperationSendingMode; NoOpInterval.

7. Syslog server port definition support:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to define the port of the Syslog server. When no port is defined, the default port of 514 is used.

Relevant parameter: SyslogServerPort.

8. Jitter Buffer defaults modified to 10 msec:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The default values for the Jitter Buffer DJBufMinDelay and DJBufOptFactor *ini* file parameters were changed to 10 msec.

Relevant parameters: DJBufMinDelay; DJBufOptFactor.

9. DTMF twist of 3 dB (TBR21 standard):

MP-112	MP-114/MP-118	MP-124	FXS	FXO

When generating a DTMF signal, a difference of 3 dB between high and low frequencies was added. In the next applicable version, the difference will be reverted back to 0 dB (configurable using new configuration parameter).

10. HangOver time setting after muting DTMF or MF from Tel /PSTN:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to define the HangOver time, which is the voice silence time (in msec) after muting DTMF or MF digits (received from the Tel / PSTN side) before sending to the IP side.

Relevant parameter: TxDTMFHangOverTime.

11. HangOver time setting after playing DTMF or MF from IP network:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to define the HangOver time, which is the voice silence time (in msec) after playing DTMF or MF digits (received as Relay from the IP side) to the Tel / PSTN side.

Relevant parameter: RxDTMFHangOverTime.

12. IP addresses support the asterisk (*) wildcard:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The asterisk (*) wildcard can now be included in IP addresses. IP addresses that are defined in the Routing tables and Manipulation tables can include the '*' wildcard, which represents any valid value from 0 to 255.

For example, 10.8.8.* represents IP addresses from 10.8.8.0 to 10.8.8.255; 10.8.*.* represents IP addresses from 10.8.0.0 to 10.8.255.255.

Relevant parameters: Prefix; PSTNPrefix; NumberMapIP2Tel; SourceNumberMapIP2Tel.

13. Additional option for Channel Selection algorithm:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

An additional option ('By Source Phone Number') was added to the channel selection algorithm (in addition to the existing 'By Destination Phone Number' option).

Relevant parameters: ChannelSelectMode; TrunkGroupSettings.

14. Support for sending CDR on call connect:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway can now send a CDR when a call is connected (in addition to when the call ends).

Relevant parameter: CDRReportLevel.

15. Supports Call Forward Indication to user:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

When a phone on an FXS port goes off-hook to make a call, the gateway typically plays a regular dial tone for a period of time, indicating that the user can dial digits. If this port has Call Forwarding active, the user needs to be aware that any calls made to their directory number (DN) are not sent to their phone. To notify users of the call forwarding status, this Call Forward Indication feature plays a stutter dial tone instead of the regular dial tone. This indicates to the user that to receive calls, the user needs to disable call forwarding.

Relevant parameter: StutterToneDuration.

16. Supports defining of Off-Hook Warning Tone duration:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

It is now possible to set the duration for which the Off-Hook Warning Tone is played.

Relevant parameter: WarningToneDuration.

17. Support for defining number of rings before FXO answers:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

It is now possible to define the number of rings before the FXO gateway answers a call.

Relevant parameter: FXONumberOfRings.

1.3 SIP New Features

1. **Support for RFC 3605 (RTCP attribute in SDP):**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports RFC 3605 (RTCP attribute in SDP). When a session requires multiple ports, SDP assumes that these ports have consecutive numbers (RTCP Port = RTP Port + 1). However, when the session crosses a NAT device that also uses port mapping, the order of ports can change by the translation. To handle this scenario, an extension attribute 'rtcp' was added. The 'rtcp' attribute documents the RTCP port used for media stream when the port is not the next higher (odd) port number following the RTP port described in the media line. The 'rtcp' attribute can include the RTCP port and a different IP address (if relevant).

2. **Support for reception of 3xx SIP messages in response to REGISTER requests:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports reception of 3xx SIP messages in response to REGISTER requests. Upon receiving a 3xx response for a REGISTER request, the Re-REGISTER is immediately sent to the new location according to the Contact header in the 3xx response. If the response is a 301 'Moved Permanently', all future REGISTER messages are sent to the new location.

3. **Support for multiple Packetization Time (Ptime) values:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

Support for multiple packetization time (Ptime) values was added. RFC 2327 (SDP) only defines a 'ptime' attribute that includes the value for the first defined coder per media line. A new SDP attribute called 'mptime' has been added in which a separate 'ptime' value is defined for each coder provided in the media line.

Relevant parameter: MultiPtimeFormat.

4. **Enhanced support for G.726 (32 kbps) coder:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

For coder G.726 (32 kbps), the gateway now supports a dynamic payload type instead of the constant one (2). In addition, support was added for rates of 16, 24, and 40 kbps.

Relevant parameters: CoderName; CoderName_ID.

5. **Support for RFC 3389 (RTP Payload for Comfort Noise):**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports RFC 3389 (RTP Payload for Comfort Noise). When using the SDP to specify RTP payload information, the use of comfort noise (CN) is indicated by including a payload type for CN on the media description line. The gateway can use CN with a codec whose RTP timestamp clock rate is 8,000 Hz (G.711/G.726). The use of CN is negotiated between sides; therefore, if the remote side does not support CN, it's not used.

Relevant parameter: ComfortNoiseNegotiation.

6. **Support for RFC 3959 (The Early Disposition Type for SIP):**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway supports RFC 3959 (The Early Disposition Type for SIP). The gateway now supports two separate Offer/Answer sessions: one for regular voice establishment; the other for an Early Media session. The gateway doesn't generate two SDP Offers, but it supports reception of two Offers and responds appropriately. To support this function, both Early Media and PRACK usage must be configured.

Relevant parameters: EnableEarlyMedia; PRACKMode.

7. **Support for ITU V.152 (Procedures for supporting Voice-Band Data over IP Networks):**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports ITU V.152 (Procedures for supporting Voice-Band Data over IP Networks). Voice Band Data (VBD) is the transport of modem, fax, and text telephony signals over a voice channel in a packet network with a codec appropriate for such signals.

The coder table configuration was enhanced to support the V.152 capability. New entries were added to indicate T.38 and VBD support (either A-law or Mu-law). All selected options are declared in the outgoing SDP when initiating calls to IP. Negotiation is performed separately on each capability -- voice coder, VBD, and T.38. After the initial negotiation, no Re-INVITEs are necessary as both sides are synchronized in terms of the other side's capabilities.

Relevant parameters: CoderName; CoderName_ID; IsFaxUsed.

8. **Support for TCP connection re-use:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports the reuse of the same TCP connection for all calls to the same destination. When disabled, each call uses a separate TCP connection.

Relevant parameter: EnableTCPConnectionReuse.

9. **Enhanced Proxy Keep-Alive mechanism:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The Proxy Keep-Alive mechanism was enhanced by using responses to INVITE requests. If the active proxy does not respond to INVITE messages sent by the gateway, the proxy is marked as offline. This capability is in addition to the use of OPTIONS or REGISTER messages.

Relevant parameter: EnableProxyKeepAlive.

10. **Support for RFC 4244 (An Extension to SIP for Request History Information):**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports RFC 4244 (An Extension to SIP for Request History Information). When enabled, History-Info headers are added and managed according to the 'history' of the call (i.e., redirection requests and / or failure responses).

Relevant parameter: EnableHistoryInfo.

11. Support for handling forking proxy multiple responses:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway can now handle forking proxy multiple responses. When passing through a forking proxy, the UAC may receive multiple 1xx / 2xx responses. The multiple responses can be identified by the usage of different remote tags. Therefore, each response that has a different remote tag (than the responses that have already arrived) is saved separately. Early Media is only established with the first received 1xx response (if necessary). The first transaction that receives a 200 OK response is the active one. For other 200 OK responses, the gateway sends an ACK and immediately afterwards, sends a BYE.

12. DNS Naming Authority Pointer (NAPTR) queries for resolving domain names:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

DNS Naming Authority Pointer (NAPTR) queries can now be used to resolve domain names of Proxy servers, Registrar servers, and any domain name that appears in the Contact and Record-Route headers.

Relevant parameters: DNSQueryType; ProxyDNSQueryType.

13. Supports Load Balancing for Proxy servers:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway can use load balancing algorithms when using Proxy servers. The load balancing can either use a Round Robin mechanism where each new request is sent to the next Proxy in the list, or use a Random Weights algorithm according to the SRV response received from the domain name system (DNS) server. When weights are used, the requests are not distributed equally among the servers, but according to the weight assigned to each server.

Relevant parameters: ProxyLoadBalancingMethod; ProxyIPListRefreshTime.

14. Supports NAPTR/SRV resolution on Routing table entries:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

If the destination IP address in the Tel2IP Routing table or the source IP address in the IP2Tel Routing table is a fully qualified domain name (FQDN), and the gateway is configured to use Naming Authority Pointer (NAPTR) and/or SRV DNS queries, then the gateway performs resolution of that FQDN according to these mechanisms.

15. Supports NAPTR/SRV resolution on multiple Contact headers in a 3xx response:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway uses DNS resolution when a 3xx response is received that includes an FQDN in the Contact header. If the FQDN is resolved into more than one IP address, the gateway first attempts to reach the first address. If no response is received and the correct Reason for Alternative Routing is configured, the gateway attempts to reach the second resolved address.

16. **Support for internal DNS SRV table:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports an internal DNS SRV table. This table is used to resolve domain names into DNS A-Records. Each record in the table includes the Transport Type (UDP, TCP or TLS), and up to three A-records. Each A-record includes a domain name, priority, weight, and port. When an SRV resolution is required, this internal DNS SRV table is searched for a match with the domain name. If found, the SRV record information is used; if not found, the query is sent to the external DNS server.

Relevant parameter: SRV2IP.

17. **Support for draft-ietf-sip-gruu-09 [Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP]:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports Internet-Draft draft-ietf-sip-gruu-09 [Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP]. A Globally Routable User Agent URI (GRUU) is a type of URI that routes to a specific UA instance and can be reached from anywhere.

The gateway obtains a GRUU by generating a normal REGISTER request. This request contains a Supported header field with the value 'gruu'. The gateway includes a '+sip.instance' Contact header field parameter for each contact for which the GRUU is desired. If the Registrar/Proxy supports GRUU, the REGISTER responses include the 'gruu' parameter in each Contact header field. In scenarios where REGISTER is sent again after expiration of the registration, the Registrar/Proxy provides the same GRUU for the same Address-of-Record (AOR) and instance-id.

The gateway includes the GRUU in any header field that contains a URI. It uses the GRUU in the following messages: INVITE requests, 2xx responses to INVITE, SUBSCRIBE requests, 2xx responses to SUBSCRIBE, NOTIFY requests, REFER requests, and 2xx responses to REFER.

Relevant parameter: EnableGRUU.

18. **Supports Registration Mode per Hunt Group:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The Registration Mode can now be configured per Hunt Group. Each Hunt Group can register as one group, or each endpoint in the Hunt Group can register separately.

Relevant parameter: TrunkGroupSettings.

19. **Supports 'q' Contact parameter:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports reception of a q-value in the Contact header. When the gateway receives a 3xx response with multiple contacts, the q-value may be added per contact. This q-value indicates the order in which the gateway should try the contacts. The gateway performs serial processing in decreasing q-value order, while keeping the original order in case of contacts of equal q-value.

20. Support for RFC 3824 [Using E.164 numbers with SIP (ENUM)]:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The E.164 Number Mapping (ENUM) system uses DNS to translate certain telephone numbers (e.g., '+97239764392') into URIs (e.g., 'sip:johndoe@audiocodes.com'). To use ENUM, the user must enter the string 'ENUM' as the destination IP address in the Tel2IP Routing table. In this scenario, the gateway sends an NAPTR request to the external DNS server to resolve the received phone number into a SIP URI. The SIP URI, which is included in the response is used as the Request-URI in the outgoing INVITE. ENUM is not used for routing purposes when Proxy is in use. When Proxy is not used, the INVITE is sent to the IP address that was received in the ENUM reply.

21. Handling of Transfer in Alerting State:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

According to Internet-Draft draft-ietf-sipping-cc-transfer-05, the transferor (party initiating transfer) may hang up before the session (to the transfer target) is established. In this scenario, the transferor may wish to proceed with the transfer action. Currently, the gateway uses Replaces in the REFER regardless of the state of the session; however, this is not allowed in the Alerting state.

When this feature is enabled, the gateway sends a CANCEL message when the transferor hangs up. Thereafter, the gateway waits for a 487 or 200 response to the INVITE. After receiving 487, the gateway sends a REFER without Replaces. However, if a 200 OK response is received, the gateway sends REFER with Replaces.

Relevant parameter: EnableSemiAttendedTransfer.

22. Supports Hook-Flash signaling using RFC 2833:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports the generation of a Hook-Flash signal using RFC 2833, in addition to the already supported proprietary INFO message. Both options can be used simultaneously. The Hook-Flash signal using RFC 2833 is also indicated in the outgoing SDP.

Relevant parameter: HookFlashOption.

23. Supports 3-way Conference Calls:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports the creation of 3-way Conference Calls using an external media server. When a specific port is involved in an active call and another call is received, destined to the same port, it's now possible to connect all three parties into a conference session. The first Hook-Flash action places the first, initial call on hold, and then answers the second call. Another Hook-Flash sends a Conference-initiating INVITE to a media server. At the same time, the gateway sends REFER messages to the two remote parties to add them as participants to the conference.

It's possible to configure the digit pattern that once detected, generates the Conference-initiating INVITE (by default, it's set to "!" = Hook-Flash). In addition, there are two different modes of operation:

- The Conference-initiating gateway provides the conference unique identifier.
- The media server provides the conference unique identifier and the gateway distributes this identifier to the remote parties in the Refer-To header of the REFER message.

Relevant parameters: Enable3WayConference; ConferenceID; ConferenceCode; 3WayConferenceMode.

24. Call Waiting for Remote Extension:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

When the FXO gateway detects a Call Waiting indication (FSK data of the Caller Id), it sends a proprietary INFO message, which includes the caller identification to the FXS gateway. Once the FXS gateway receives this INFO message, it forwards the information to the relevant port for display.

1.4 Web and SNMP New Features

1. Supports Graceful/Forced Lock and Reset:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports a lock/unlock mechanism. The user can select one of the following options:

- Graceful Lock: the gateway rejects all incoming calls. All existing calls are allowed to continue until a user-defined lock timer expires. When this timer expires, the gateway disconnects the calls. At this point, the gateway remains in an idle state.
- Forced Lock: the gateway rejects all incoming calls and all existing calls are disconnected. At this point the gateway remains in an idle state.
- Unlock: the gateway returns from Lock state to normal state and accepts incoming calls from Tel and IP sides.
- Graceful Reset: same behavior as Graceful Lock only that when all calls are disconnected, the gateway performs reset.
- Forced Reset: same behavior as Forced Lock only that when all calls are disconnected, the gateway performs reset.

2. **Support for assigning free-text description for each port:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

This feature allows users to assign free-text descriptions for each port via the gateway's Embedded Web Server.

3. **Web Search Engine support:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway's Embedded Web Server now provides a search engine (Search button) for searching any ini file parameter that is configurable by the Web server. The search result provides you a brief description of the parameter as well as a link to the relevant screen in which the parameter is configured in the Web server.

The search can be performed for a specific *ini* parameter (e.g., EnableIPSec) or a sub-string of the parameter (e.g., 'sec'). If you search for a sub-string, the Embedded Web Server lists all parameters that contain the searched sub-string in their parameter names.

4. **SNMPv3 support:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

In previous releases, it was assumed that customers could use SNMPv2c over IPsec to meet their SNMP security requirements. While SNMP over IPsec is a viable solution for some customers, others however, demand SNMPv3 security. Therefore, in Release 5.0, support for SNMPv3 authentication and privacy has been provided.

This feature allows customers to define up to 10 User-based Security Model (USM) users (USM users are referred to as 'v3 users'). Each v3 user can be associated with an authentication type (none, MD5, or SHA-1) and a privacy type (none, DES, 3DES, or AES).

The customer still has the option for defining up to five read-only community strings and up to five read-write community strings.

Relevant parameters: SNMPUsers_Index; SNMPUsers_Username; SNMPUsers_AuthProtocol; SNMPUsers_PrivProtocol; SNMPUsers_AuthKey; SNMPUsers_PrivKey; SNMPUsers_Group.

1.5 Resolved Constraints

N/A.

1.6 New Parameters

Most new parameters (described in Table 1-1) can be configured with the *ini* file and via the Embedded Web Server. Note that only those parameters contained within square brackets are configurable via the Embedded Web Server.

Table 1-1: Release 5.0 New *ini* File [Web Browser] Parameters (continues on pages 18 to 24)

***ini* File [Web Interface] Parameter Name**	**Description**
MaxEchoCancellerLength [Max Echo Canceller Length]	Maximum Echo Canceller length (in msec). Valid options include: ▪ 0 = based on various internal gateway settings -- 64 msec (default) ▪ 4 = 32 msec ▪ 11 = 64 msec **Note 1:** The gateway must be reset after the value of 'MaxEchoCancellerLength' is changed. **Note 2:** It is unnecessary to configure the parameter EchoCancellerLength as it automatically acquires its value from the parameter MaxEchoCancellerLength.
NTTDIDSignallingForm	Determines the type of Direct Inward Dialing (DID) signaling support for NTT (Japan) modem: DTMF- or Frequency Shift Keying (FSK)-based signaling. Gateways can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX. Valid options include: ▪ 0 = FSK-based signaling (default) ▪ 1 = DTMF-based signaling **Note:** Applicable only to FXS gateways.
NoOperationSendingMode	Enables or disables the transmission of RTP or T.38 No-Op packets. Valid options include: ▪ 0 = Disable (default) ▪ 1 = Enable This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.
NoOpInterval	Defines the time interval in which RTP or T.38 No-Op packets are sent in the case of silence (no RTP / T.38 traffic) when No-Op packet transmission is enabled. The valid range is 20 to 65,000 msec. The default is 10,000. **Note:** To enable No-Op packet transmission, use the NoOperationSendingMode parameter.
SyslogServerPort [Syslog Server Port]	Defines the UDP port of the Syslog server. The valid range is 0 to 65,535. The default port value is 514.
PPPoELCPEchoEnable	Enables or disables the Point-to-Point Protocol over Ethernet (PPPoE) disconnection auto-detection feature. Valid options include: ▪ 0 = Disable ▪ 1 = Enable (default) By default, the PPPoE Client (i.e., embedded in the gateway) sends LCP Echo packets to the server to check that the PPPoE connection is open. Some Access Concentrators (PPPoE servers) don't reply to these LCP Echo requests, resulting in a disconnection. By disabling the LCP disconnection auto-detection feature, the PPPoE Client does not send LCP Echo packets to the server (and does not detect PPPoE disconnections).
RxDTMFHangOverTime	Defines the Voice Silence time (in msec) after playing DTMF or MF digits to the Tel / PSTN side that arrive as Relay from the IP side. The valid range is 0 to 2,000 msec. The default is 1,000 msec.

Table 1-1: Release 5.0 New *ini* File [Web Browser] Parameters (continues on pages 18 to 24)

ini File [Web Interface] Parameter Name	Description
TxDTMFHangOverTime	Defines the Voice Silence time (in msec units) after detecting the end of DTMF or MF digits at the Tel / PSTN side when the DTMF Transport Type is either Relay or Mute. The Valid range is 0 to 2,000 msec. The default is 100 msec.
STUNServerDomainName	Defines the domain name for the STUN server's address (for retrieving all STUN servers with an SRV query). The STUN client can perform the required SRV query to resolve this domain name to an IP address and port, sort the server list, and use the servers according to the sorted list. **Note:** Use either the STUNServerPrimaryIP or STUNServerDomainName method, with priority to the former one.
SNMP V3 Settings	
SNMPUsers_Index [Index]	SNMP v3 user table index. The valid range is 0 to 9.
SNMPUsers_Username [Username]	Name of the SNMP v3 user. This name must be unique.
SNMPUsers_AuthProtocol [AuthProtocol]	Authentication protocol for the SNMP v3 user. Valid options include: ▪ 0 = None (default) ▪ 1 = MD5 ▪ 2 = SHA-1
SNMPUsers_PrivProtocol [PrivProtocol]	Privacy protocol for the SNMP v3 user. Valid options include: ▪ 0 = None (default) ▪ 1 = DES ▪ 2 = 3DES ▪ 3 = AES128 ▪ 4 = AES192 ▪ 5 = AES256
SNMPUsers_AuthKey [AuthKey]	Authentication key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
[SNMPUsers_PrivKey [PrivKey]	Privacy key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
SNMPUsers_Group [Group]	The group with which the SNMP v3 user is associated. Valid options include: ▪ 0 = Read-only group (default) ▪ 1 = Read-write group ▪ 2 = Trap group **Note:** All groups can be used to send traps.
SIP Parameters	
ComfortNoiseNegotiation [Comfort Noise Generation Negotiation]	Enables negotiation and usage of Comfort Noise (CN). Valid options include: ▪ 0 = Disable (default) ▪ 1 = Enable Comfort Noise negotiation The use of CN is indicated by including a payload type for CN on the media description line of the SDP. The gateway can use CN with a codec whose RTP timestamp clock rate is 8,000 Hz (G.711/G.726). The static payload type 13 is used. The use of CN is negotiated between sides; therefore, if the remote side doesn't support CN, it is not used. **Note:** Silence Suppression must be enabled to generate CN.

Table 1-1: Release 5.0 New *ini* File [Web Browser] Parameters (continues on pages 18 to 24)

***ini* File [Web Interface] Parameter Name**	**Description**
EnableReasonHeader [Enable Reason Header]	Enables or disables the usage of the SIP Reason header. Valid options include: ▪ 0 = Disable ▪ 1 = Enable (default)
ProxyDNSQueryType [Proxy DNS Query Type]	Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers. Valid options include: ▪ 0 = A-Record (default) ▪ 1 = SRV ▪ 2 = NAPTR If set to A-Record (0), no NAPTR or SRV queries are performed. If set to SRV (1) and the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com), an SRV query is performed. The SRV query returns up to four Proxy host names and their weights. The gateway then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names, and the A-record queries return two IP addresses each, no more searches are performed. If set to NAPTR (2), an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type. If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the gateway performs a regular DNS A-record query. **Note:** When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.
DNSQueryType [DNS Query Type]	Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to resolve Proxy and Registrar servers and to resolve all domain names that appear in the Contact and Record-Route headers. Valid options include: ▪ 0 = A-Record (default) ▪ 1 = SRV ▪ 2 = NAPTR If set to A-Record (0), no NAPTR or SRV queries are performed. If set to SRV (1), and the Proxy / Registrar IP address parameter or the domain name in the Contact / Record-Route headers contains a domain name without port definition, an SRV query is performed. The gateway uses the first host name received from the SRV query. The gateway then performs DNS A-record query for the host name to locate an IP address. If set to NAPTR (2), an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type. If the Proxy / Registrar IP address parameter or the domain name in the Contact / Record-Route headers contains a domain name with port definition, the gateway performs a regular DNS A-record query. **Note:** To enable NAPTR/SRV queries only for Proxy servers, use the parameter ProxyDNSQueryType.

Table 1-1: Release 5.0 New *ini* File [Web Browser] Parameters (continues on pages 18 to 24)

***ini* File [Web Interface] Parameter Name**	**Description**
ProxyLoadBalancingMethod [Proxy Load Balancing Method]	Enables the usage of the Proxy Load Balancing mechanism. Valid options include: ▪ 0 = Load Balancing is disabled (default) ▪ 1 = Round Robin ▪ 2 = Random Weights When Round Robin (1) algorithm is used, a list of all possible Proxy IP addresses is compiled. This list includes all entries in the ProxyIP table after necessary DNS resolutions (including NAPTR and SRV, if configured). This list can handle up to 15 entries. After this list is compiled, the Proxy Keep-Alive mechanism (according to EnableProxyKeepAlive and ProxyKeepAliveTime) is used to mark each entry as Offline or Online. The balancing is only performed on Proxy servers that are marked as Online. All outgoing messages are equally distributed across the Proxy IP list. REGISTER messages are also distributed unless a RegistrarIP is configured. The Proxy IP list is refreshed according to ProxyIPListRefreshTime. If a change in the order of the entries in the list occurs, all load statistics are erased and balancing starts over again. When Random Weights (2) algorithm is used, the outgoing requests are not distributed equally among the Proxies. The weights are received from the DNS server by using SRV records. The gateway sends the requests in such a fashion that each Proxy receives a percentage of the requests according to its assigned weight. Load Balancing is not used in the following scenarios: ▪ The ProxyIP table includes more than one entry. ▪ The only Proxy defined is an IP address and not an FQDN. ▪ SRV usage is not enabled (DNSQueryType). ▪ The SRV response includes several records with a different Priority value.
ProxyIPListRefreshTime [Proxy IP List Refresh Time]	Defines the time interval (in seconds) between refreshes of the Proxy IP list. This parameter is used only when ProxyLoadBalancingMethod = 1. The interval range is 5 to 2,000,000. The default interval is 60.

Table 1-1: Release 5.0 New *ini* File [Web Browser] Parameters (continues on pages 18 to 24)

<table>
<tr><th>*ini* File [Web Interface] Parameter Name</th><th>Description</th></tr>
<tr><td>EnableHistoryInfo
[Enable History-Info Header]</td><td>Enables usage of the History-Info header.
Valid options include:
▪ 0 = Disable (default)
▪ 1 = Enable

UAC Behavior:
▪ Initial request: The History-Info header is equal to the Request URI. If a PSTN Redirect number is received, it is added as an additional History-Info header with an appropriate reason.
▪ Upon receiving the final failure response, the gateway copies the History-Info as is, adds the reason of the failure response to the last entry, and concatenates a new destination to it (if an additional request is sent).
The order of the reasons is as follows:
- Q.850 Reason
- SIP Reason
- SIP Response code
▪ Upon receiving the final (success or failure) response, the gateway searches for a Redirect reason in the History-Info (i.e., 3xx/4xx SIP Reason). If found, it is passed to ISDN, according to the following table:
<table>
<tr><th>SIP Reason Code</th><th>ISDN Redirecting Reason</th></tr>
<tr><td>302 – Moved Temporarily</td><td>Call Forward Universal (CFU)</td></tr>
<tr><td>408 – Request Timeout</td><td rowspan="3">Call Forward No Answer (CFNA)</td></tr>
<tr><td>480 – Temporarily Unavailable</td></tr>
<tr><td>487 – Request Terminated</td></tr>
<tr><td>486 – Busy Here</td><td rowspan="2">Call Forward Busy (CFB)</td></tr>
<tr><td>600 – Busy Everywhere</td></tr>
</table>
▪ If history reason is a Q.850 reason, it is translated to the SIP reason (according to the SIP-ISDN tables) and then to ISDN Redirect reason according to the table above.
UAS Behavior:
▪ History-Info is sent in the final response only.
▪ Upon receiving a request with History-Info, the UAS checks the policy in the request. If 'session', 'header', or 'history' policy tag is found, the (final) response is sent without History-Info. Otherwise, it is copied from the request.</td></tr>
<tr><td>HookFlashCode
[Hook-Flash Code]</td><td>Determines a digit pattern which, when received from the Tel side, indicates a Hook Flash event.
The valid range is a 25-character string.</td></tr>
<tr><td>EnableTCPConnectionReuse
[Enable TCP Connection Reuse]</td><td>Enables the reuse of the same TCP connection for all calls to the same destination.
Valid options include:
▪ 0 = Use a separate TCP connection for each call (default)
▪ 1 = Use the same TCP connection for all calls</td></tr>
</table>

Table 1-1: Release 5.0 New *ini* File [Web Browser] Parameters (continues on pages 18 to 24)

***ini* File [Web Interface] Parameter Name**	**Description**
MultiPtimeFormat [Multiple Packetization Time Format]	Determines whether the 'mptime' attribute is included in the outgoing SDP. Valid options include: ▪ 0 = Disable (default) ▪ 1 = Enable (includes the mptime attribute in the outgoing SDP -- PacketCable defined format) The 'mptime' attribute enables the IP gateway to define a separate Packetization period for each negotiated coder in the SDP. The 'mptime' attribute is only included if this parameter is enabled, even if the remote side includes it in the SDP offer. Upon reception, each coder receives its 'ptime' value in the following precedence: From 'mptime' attribute. From 'ptime' attribute. Default value.
SRV2IP [Internal SRV Table]	Defines the internal SRV table used for resolving host names to DNS A-Records. Three different A-Records can be assigned to a hostname. Each A-Record contains the host name, priority, weight, and port. SRV2IP = <Internal Domain Name>, <Transport Type>, <DNS Name 1>, <Priority 1>, <Weight 1>, <Port 1>, <DNS Name 2>, <Priority 2>, <Weight 2>, <Port 2>, <DNS Name 3>, <Priority 3>, <Weight 3>, <Port 3> **Note 1**: If the internal SRV table is configured, the gateway first tries to resolve a domain name using this table. If the domain name isn't found, the gateway performs an SRV resolution using an external DNS server. **Note 2**: This parameter can appear up to 10 times.
EnableGRUU [Enable GRUU]	Determines whether or not the Globally Routable User Agent (GRUU) mechanism is used. Valid options include: ▪ 0 = Disable (default) ▪ 1 = Enable The gateway obtains a GRUU by generating a normal REGISTER request. If the Registrar/Proxy supports GRUU, the REGISTER responses contain the "gruu" parameter in each Contact header field. The gateway includes the GRUU in any header field that contains a URI. It uses the GRUU in the following messages: INVITE requests, 2xx responses to INVITE, SUBSCRIBE requests, 2xx responses to SUBSCRIBE, NOTIFY requests, REFER requests, and 2xx responses to REFER. **Note:** If the GRUU contains the 'opaque' URI parameter, the gateway obtains the Address-of-Record (AOR) for the user by stripping the parameter. The resulting URI is the AOR. For example: AOR: sip:alice@example.com GRUU: sip:alice@example.com;opaque="kjh29x97us97d"
EnableSemiAttendedTransfer [Enable Semi-Attended Transfer]	Determines the gateway's behavior when Transfer is initiated while still in Alerting state. Valid options include: ▪ 0 = Send REFER with Replaces (default) ▪ 1 = Send CANCEL, and after a 487 response is received, send REFER without Replaces

Table 1-1: Release 5.0 New *ini* File [Web Browser] Parameters (continues on pages 18 to 24)

ini File [Web Interface] Parameter Name	Description
HookFlashOption [Hook-flash Option]	Supported hook-flash Transport Type (method by which hook-flash is sent and received). Valid options include: ▪ 0 = Hook-Flash indication isn't sent (default) ▪ 1 = Send proprietary INFO message with Hook-Flash indication ▪ 4 = RFC 2833 **Note:** FXO gateways support the receiving of RFC 2833 Hook-Flash signals.
Enable3WayConference [Enable 3-Way Conference]	Enables or disables the 3-Way Conference feature. Valid options include: ▪ 0 = Disable (default) ▪ 1 = Enable
ConferenceID [Conference ID]	Defines the Conference Identification string (up to 16 characters). The gateway uses this identifier in the Conference-initiating INVITE that is sent to the media server when Enable3WayConferenceis set to 1. The default value is 'conf'. For example: ConferenceID = MyConference.
ConferenceCode [Establish Conference Code]	Defines the digit pattern that once detected, generates the Conference-initiating INVITE when Enable3WayConference is set to 1. The valid range is a 25-character string. The default is "!" (Hook-Flash).
3WayConferenceMode	Defines the mode of operation when the 3-Way Conference feature is used. Valid options include: ▪ 0 = Conference-initiating INVITE (sent by the gateway), uses the ConferenceID concatenated with a unique identifier as the Request-UR (default) ▪ 1 = Conference-initiating INVITE (sent by the gateway), uses only the ConferenceID as the Reques-URI If 3wayConferenceMode is set to 0, the Conference-initiating INVITE sent by the gateway, uses the ConferenceID concatenated with a unique identifier as the Request-URI. This same Request-URI is set as the Refer-To header value in the REFER messages that are sent to the two remote parties. If 3wayConferenceMode is set to 1, the Conference-initiating INVITE sent by the gateway, only uses the ConferenceID as the Reques-URI. The media server sets the Contact header of the 200 OK response to the actual unique identifier (Conference URI) to be used by the participants. This Conference URI is included (by the gateway), in the Refer-To header value in the REFER messages sent by the gateway to the remote parties. The remote parties join the conference by sending INVITE messages to the media server using this conference URI.
WarningToneDuration	Defines the duration (in seconds) for which Off-Hook Warning Tone is played to the user. The valid range is -1 to 2,147,483,647 seconds. The default is 600 seconds. **Note**: A negative value indicates that the tone is played infinitely.
FXONumberOfRings	Defines the number of rings before the FXO gateway answers a call. The valid range is 0 to 255. The default is 0 seconds.

1.7 Modified Parameters

Table 1-2 lists existing parameters that have been modified. Note that only those parameters contained within square brackets are configurable via the Embedded Web Server.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

<table>
<tr><th>ini File [Web Interface] Parameter Name</th><th>Description</th></tr>
<tr><td>DJBufMinDelay
[Dynamic Jitter Buffer Minimum Delay]</td><td>(Modification: default value.)
Minimum delay for the Dynamic Jitter Buffer.
The valid range is 0 to 150 msec (default is 10).</td></tr>
<tr><td>DJBufOptFactor
[Dynamic Jitter Buffer Optimization Factor]</td><td>(Modification: default value.)
Dynamic Jitter Buffer frame error / delay optimization factor.
The valid range is 0 to 13 (default is 10).
Note: Set to 13 for data (fax and modem) calls.</td></tr>
<tr><td>IKEPolicyProposalEncryption_X
[First to Fourth Proposal Encryption Type]</td><td>(Modification: additional enumeration value for AES support.)
Determines the encryption type used in the main mode negotiation for up to four proposals. 'X' denotes the proposal number (0 to 3).
Valid options include:
▪ Not Defined (default)
▪ 1 = DES-CBC
▪ 2 = Triple DES-CBC
▪ 3 = AES</td></tr>
<tr><td>IPSecPolicyProposalEncryption_X
[First to Fourth Proposal Encryption Type]</td><td>(Modification: additional enumeration value for AES support.)
Determines the encryption type used in the quick mode negotiation for up to four proposals. 'X' denotes the proposal number (0 to 3).
Valid options include:
▪ Not Defined (default)
▪ 0 = None (no encryption)
▪ 1 = DES-CBC
▪ 2 = Triple DES-CBC
▪ 3 = AES</td></tr>
<tr><td>CoderName</td><td>(Modification: Support for additional coders: T.38, G.711A-law_VBD, and G.711U-law_VBD. G.726 payload type and rate modified.)
Defines the gateway's coder list (up to five coders can be configured).
Enter coders in the following format:
CoderName=<Coder Name>,<Ptime>,<Rate>,<Payload Type>,<Silence Suppression Mode>.
<table>
<tr><th>Coder Name</th><th>Packetization Time</th><th>Rate</th><th>Payload Type</th><th>Silence Suppression</th></tr>
<tr><td>G.711 A-law [g711Alaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 8</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.711 μ-law [g711Ulaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 0</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.729 [g729]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100</td><td>Always 8</td><td>Always 18</td><td>Disable [0]
Enable [1]
Enable w/o Adaptations [2]</td></tr>
</table>
</td></tr>
</table>

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

<table>
<tr><th>ini File [Web Interface] Parameter Name</th><th colspan="5">Description</th></tr>
<tr><td></td><td>G.723.1 [g7231]</td><td>30 (default), 60, 90, 120</td><td>5.3 [0], 6.3 [1] (default)</td><td>Always 4</td><td>Disable [0] Enable [1]</td></tr>
<tr><td></td><td>G.726 [g726]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>16 [0], 24 [1], 32 [2] (default), 40 [3]</td><td>Dynamic (0-120)</td><td>Disable [0] Enable [1]</td></tr>
<tr><td></td><td>T.38 [t38fax]</td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr>
<tr><td></td><td>G.711A-law_VBD [g711AlawVbd]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Dynamic (0-120)</td><td>N/A</td></tr>
<tr><td></td><td>G.711U-law_VBD [g711UlawVbd]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Dynamic (0-120)</td><td>N/A</td></tr>
<tr><td></td><td colspan="5">Note 1: The coder name is case-sensitive.
Note 2: If silence suppression is not defined (for a specific coder), the value defined by the parameter EnableSilenceCompression is used.
Note 3: The value of several fields is hard-coded according to well-known standards (e.g., the payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored.
For example:
CoderName = g711Alaw64k,20,,,0
CoderName = g711Ulaw64k,40
CoderName = g7231,90,1,,1
CoderName = g726,$$,2,,0</td></tr>
<tr><td>CoderName_ID</td><td colspan="5">(Modification: Support for additional coders: T.38, G.711A-law_VBD, and G.711U-law_VBD. G.726 payload type and rate modified.)
Defines groups of coders that can be associated with IP or Tel profiles (up to five coders in each group).
Enter coder groups in the following format:
CoderName_<coder group ID from 1 to 4>=<Coder Name>,<Ptime>,<Rate>,<Payload Type>,<Silence Suppression Mode>.</td></tr>
<tr><td></td><td>Coder Name</td><td>Packetization Time</td><td>Rate</td><td>Payload Type</td><td>Silence Suppression</td></tr>
<tr><td></td><td>G.711 A-law [g711Alaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 8</td><td>Disable [0] Enable [1]</td></tr>
<tr><td></td><td>G.711 μ-law [g711Ulaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 0</td><td>Disable [0] Enable [1]</td></tr>
<tr><td></td><td>G.729 [g729]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100</td><td>Always 8</td><td>Always 18</td><td>Disable [0] Enable [1] Enable w/o Adaptations [2]</td></tr>
<tr><td></td><td>G.723.1 [g7231]</td><td>30 (default), 60, 90, 120</td><td>5.3 [0], 6.3 [1] (default)</td><td>Always 4</td><td>Disable [0] Enable [1]</td></tr>
<tr><td></td><td>G.726 [g726]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>16 [0], 24 [1], 32 [2] (default), 40 [3]</td><td>Dynamic (0-120)</td><td>Disable [0] Enable [1]</td></tr>
<tr><td></td><td>T.38 [t38fax]</td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr>
</table>

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

ini File [Web Interface] Parameter Name	Description				
	G.711A-law_VBD [g711AlawVbd]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Dynamic (0-120)	N/A
	G.711U-law_VBD [g711UlawVbd]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Dynamic (0-120)	N/A
	Note 1: This parameter (CoderName_ID) can appear up to 20 times (five coders in four coder groups). **Note 2:** The coder name is case-sensitive. **Note 3:** If silence suppression is not defined (for a specific coder), the value defined by the parameter EnableSilenceCompression is used. **Note 4:** The value of several fields is hard-coded according to well-known standards (e.g., the payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored. For example: CoderName_1 = g711Alaw64k,20,,,0 CoderName_1 = g711Ulaw64k,40 CoderName_1 = g7231,90,1,,1 CoderName_2 = g726,$$,2,,0				
NumberMapIP2Tel	(**Modification:** asterisk ('*') wildcard supported in IP addresses.) Manipulates the destination number for IP to Tel calls. The format for NumberMapIP2Tel is as follows: a,b,c,d,e,f,g,h,i Where, ▪ a = Destination number prefix. ▪ b = Number of stripped digits from the left, or (if brackets are used) from the right. A combination of both options is allowed. ▪ c = String to add as prefix, or (if brackets are used) as suffix. A combination of both options is allowed. ▪ d = Number of remaining digits from the right. ▪ e = Not applicable, set to $$. ▪ f = Not applicable, set to $$. ▪ g = Source number prefix. ▪ h = Not applicable, set to $$. ▪ i = Source IP address (obtained from the Contact header in the INVITE message). The 'b' to 'd' manipulation rules are applied if the called and calling numbers match the 'a', 'g' and 'i' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign '$$', for example: ▪ NumberMapIP2Tel =01,2,972,$$,$$,$$,034,$$,10.13.77.8 ▪ NumberMapIP2Tel =03,(2),667,$$,$$,$$,22 **Note:** The Source IP address can include wildcards. The 'x' wildcard is used to represent single digits, e.g. 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g. 10.8.8.* represents all the addresses between 10.8.8.0 and 10.8.8.255.				

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

ini File [Web Interface] Parameter Name	Description
SourceNumberMapIP2Tel	(**Modification:** asterisk ('*') wildcard supported in IP addresses.) Manipulates the source number for IP to Tel calls. The format for SourceNumberMapIP2Tel is as follows: a,b,c,d,e,f,g,h,I Where, ▪ Source number prefix ▪ b = Number of stripped digits from the left, or (if brackets are used) from the right. A combination of both options is allowed. ▪ c = String to add as prefix, or (if brackets are used) as suffix. A combination of both options is allowed. ▪ d = Number of remaining digits from the right ▪ e = Not in use, should be set to $$ ▪ f = Not in use, should be set to $$ ▪ g = Destination number prefix ▪ h = Not in use, should be set to $$ ▪ I = Source IP address (obtained from the Request-URI in the INVITE message). The 'b' to 'd' manipulation rules are applied if the called and calling numbers match the 'a', 'g' and 'I' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign '$$', for example: ▪ SourceNumberMapIP2Tel =01,2,972,$$,$$,$$,034 ▪ SourceNumberMapIP2Tel =03,(2),667,$$,$$,$$,22 **Note:** The Source IP address can include wildcards. The 'x' wildcard is used to represent single digits, e.g. 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g. 10.8.8.* represents all the addresses between 10.8.8.0 and 10.8.8.255.
Prefix	(**Modification:** asterisk ('*') wildcard supported in IP addresses.) Prefix = <Destination Phone Prefix>, <IP Address>,<Src Phone Prefix>,<IP Profile ID>,<Charge Code> For example: Prefix = 20,10.2.10.2,202,1,15 Prefix = 10[340-451]xxx#,10.2.10.6,*,1,1 Prefix = *,gateway.domain.com,*,20 **Note 1:** <destination / source phone prefix> can be single number or a range of numbers. **Note 2:** This parameter can appear up to 50 times. **Note 3:** Parameters can be skipped by using the sign '$$', for example: Prefix = $$,10.2.10.2,202,1 **Note 4:** An optional IP ProfileID (1 to 9) can be applied to each routing rule. **Note 5:** The IP address can include wildcards. The '*' wildcard represents any number between 0 and 255, e.g., 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

ini File [Web Interface] Parameter Name	Description
PSTNPrefix	(**Modification:** asterisk ('*') wildcard supported in IP addresses.) The format for PSTNPrefix is as follows: a,b,c,d,e Where, ▪ a = Destination Number Prefix ▪ b = Hunt Group ID ▪ c = Source Number Prefix ▪ d = Source IP address (obtained from the Contact header in the INVITE message) ▪ e = IP Profile ID Selection of hunt groups (for IP to Tel calls) is according to destination number, source number and source IP address. **Note 1:** To support the 'in call alternative routing' feature, users can use two entries that support the same call, but assigned it with a different hunt groups. The second entree functions as an alternative selection if the first rule fails as a result of one of the release reasons listed in the AltRouteCauseIP2Tel table. **Note 2:** An optional IP ProfileID (1 to 4) can be applied to each routing rule. **Note 3:** The Source IP Address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g., 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. **Note 5:** This parameter can appear up to 24 times.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

ini File [Web Interface] Parameter Name	Description
ChannelSelectMode [Channel Select Mode]	(**Modification:** additional enumeration value for 'By Source Phone Number' for selecting port.) Defines common rule for port allocation of IP-to-Tel calls. Valid options include: ▪ 0 = (By phone number) Select the gateway port according to the called number (called number is defined in the 'Endpoint Phone Number' table). ▪ 1 = (Cyclic Ascending) Select the next available channel in an ascending cycle order. Always select the next higher channel number in the hunt group. When the gateway reaches the highest channel number in the hunt group, it selects the lowest channel number in the hunt group and then starts ascending again. ▪ 2 = (Ascending) Select the lowest available channel. Always start at the lowest channel number in the hunt group and if that channel is not available, select the next higher channel. ▪ 3 = (Cyclic Descending) Select the next available channel in descending cycle order. Always select the next lower channel number in the hunt group. When the gateway reaches the lowest channel number in the hunt group, it selects the highest channel number in the hunt group and then starts descending again. ▪ 4 = (Descending) Select the highest available channel. Always start at the highest channel number in the hunt group and if that channel is not available, select the next lower channel. ▪ 5 = (Number + Cyclic Ascending) First select the gateway port according to the called number (called number is defined in the 'Endpoint Phone Number' table). If the called number isn't found, then select the next available channel in ascending cyclic order. Note that if the called number is found, but the port associated with this number is busy, the call is released. ▪ 6 = (By Source Phone Number) Select the gateway port according to the calling number. The default method is 'By Phone Number'..

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

ini File [Web Interface] Parameter Name	Description
TxDTMFOption [1st to 5th Tx DTMF Option]	(**Modification:** enumeration order and default value.) Determines a single or several preferred transmit DTMF negotiation methods. Valid options include: ▪ 0 (Not Supported) = No negotiation, DTMF digits are sent according to the parameters DTMFTransportType and RFC2833PayloadType. ▪ 1 (INFO Nortel) = Sends DTMF digits according to IETF <draft-choudhuri-sip-info-digit-00>. ▪ 2 (NOTIFY) = Sends DTMF digits according to <draft-mahy-sipping-signaled-digits-01>. ▪ 3 (INFO Cisco) = Sends DTMF digits according to Cisco format. ▪ 4 (RFC 2833) -- default. **Note 1:** DTMF negotiation methods are prioritized according to the order of their appearance. **Note 2:** When out-of-band DTMF transfer is used (1, 2 or 3), the parameter DTMFTransportType is automatically set to 0 (DTMF digits are erased from the RTP stream). **Note 3:** When RFC 2833 (4) is selected, the gateway: ▪ Negotiates RFC 2833 Payload Type (PT) using local and remote SDPs. ▪ Sends DTMF packets using RFC 2833 PT according to the PT in the received SDP. ▪ Expects to receive RFC 2833 packets with the same PT as configured by the parameter RFC2833PayloadType. ▪ Uses the same PT for send and receive if the remote party doesn't include the RFC 2833 DTMF PT in its SDP. **Note 4:** When TxDTMFOption is set to 0, the RFC 2833 PT is set according to the parameter RFC2833PayloadType for both transmit and receive. ***ini* file note:** The DTMF transmit methods are defined using a repetition of the same (TxDTMFOption) parameter (up to five options can be provided).
3xxBehavior [3xx Behavior]	(**Modification:** Added Web support) Determines the gateway's behavior when a 3xx response is received for an outgoing INVITE request. The gateway can either use the same call identifiers (CallID, branch, to and from tags) or change them in the new initiated INVITE. Valid options include: ▪ 0 (forward) = Use different call identifiers for a redirected INVITE message (default). ▪ 1 (redirect) = Use the same call identifiers.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

ini File [Web Interface] Parameter Name	Description
EnableProxyKeepAlive [Enable Proxy Keep Alive]	(**Modification:** Note 3 for Proxy Keep-Alive responses to INVITE requests.) Valid options include: ▪ 0 (Disable) = Disable (default). ▪ 1 (Using OPTIONS) = Enable Keep alive with Proxy using OPTIONS. ▪ 2 (Using REGISTER) = Enable Keep alive with Proxy using REGISTER. If EnableProxyKeepAlive = 1, SIP OPTIONS message is sent every ProxyKeepAliveTime. If EnableProxyKeepAlive = 2, SIP REGISTER message is sent every RegistrationTime. Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is correctly communicating. **Note 1:** This parameter must be set to 1 (OPTIONS) when Proxy redundancy is used. **Note 2:** When EnableProxyKeepAlive = 2 (REGISTER), the homing redundancy mode is disabled. **Note 3:** When the active proxy does not respond to INVITE messages sent by the gateway, the proxy is marked as offline. The behavior is similar to a Keep-Alive (OPTIONS or REGISTER) failure.
ProxyIP [Proxy IP Address]	(**Modification:** EnableProxySRVQuery changed to ProxyDNSQueryType. Added NAPTR support.) IP address (and optionally port number) of the primary Proxy server you are using. Enter the IP address as FQDN or in dotted format notation (for example 201.10.8.1). You can also specify the selected port in the format: <IP Address>:<port>. This parameter is applicable only if you select 'Yes' in the 'Is Proxy Used' field. If you enable Proxy Redundancy (by setting EnableProxyKeepAlive=1 or 2), the gateway can work with up to four Proxy servers. If there is no response from the primary Proxy, the gateway tries to communicate with the redundant Proxies. When a redundant Proxy is found, the gateway either continues working with it until the next failure occurs or reverts to the primary Proxy (refer to the 'Redundancy Mode' parameter). If none of the Proxy servers respond, the gateway goes over the list again. The gateway also provides real time switching (hotswap mode), between the primary and redundant proxies ('IsProxyHotSwap=1'). If the first Proxy doesn't respond to INVITE message, the same INVITE message is immediately sent to the second Proxy. **Note 1:** If 'EnableProxyKeepAlive=1 or 2', the gateway monitors the connection with the Proxies by using keep-alive messages (OPTIONS or REGISTER). **Note 2:** To use Proxy Redundancy, you must specify one or more redundant Proxies using multiple 'ProxyIP= <IP address>' definitions. **Note 3:** When port number is specified (e.g., domain.com:5080), DNS SRV queries aren't performed, even if 'ProxyDNSQueryType' is set to 1.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

***ini* File [Web Interface] Parameter Name**	**Description**
First Redundant Proxy IP Address **[ProxyIP]**	(**Modification:** EnableProxySRVQuery changed to ProxyDNSQueryType. Added NAPTR support.) IP addresses of the first redundant Proxy you are using. Enter the IP address as FQDN or in dotted format notation (for example 192.10.1.255). You can also specify the selected port in the format: <IP Address>:<port>. **Note 1:** This parameter is available only if you select 'Use Proxy' in the 'Enable Proxy' field. **Note 2:** When port number is specified, DNS NAPTR/SRV queries aren't performed, even if 'ProxyDNSQueryType' is set to 1. ***ini* file note:** The IP address of the first redundant Proxy is defined by the second repetition of the *ini* file parameter 'ProxyIP'.
Second Redundant Proxy IP Address **[ProxyIP]**	(**Modification:** EnableProxySRVQuery changed to ProxyDNSQueryType. Added NAPTR support.) IP addresses of the second redundant Proxy you are using. Enter the IP address as FQDN or in dotted format notation (for example 192.10.1.255). You can also specify the selected port in the format: <IP Address>:<port>. **Note 1:** This parameter is available only if you select 'Use Proxy' in the 'Enable Proxy' field. **Note 2:** When port number is specified, DNS NAPTR/SRV queries aren't performed, even if 'ProxyDNSQueryType' is set to 1. ***ini* file note:** The IP address of the second redundant Proxy is defined by the third repetition of the *ini* file parameter 'ProxyIP'.
Third Redundant Proxy IP Address **[ProxyIP]**	(**Modification:** EnableProxySRVQuery changed to ProxyDNSQueryType. Added NAPTR support.) IP addresses of the third redundant Proxy you are using. Enter the IP address as FQDN or in dotted format notation (for example 192.10.1.255). You can also specify the selected port in the format: <IP Address>:<port>. **Note 1:** This parameter is available only if you select 'Use Proxy' in the 'Enable Proxy' field. **Note 2:** When port number is specified, DNS NAPTR/SRV queries aren't performed, even if 'ProxyDNSQueryType' is set to 1. ***ini* file note:** The IP addresses of the third redundant Proxy is defined by the fourth repetition of the *ini* file parameter 'ProxyIP'.
RegistrarIP [Registrar IP Address]	(**Modification:** EnableProxySRVQuery changed to ProxyDNSQueryType. Added NAPTR support.) IP address and optionally port number of Registrar server. Enter the IP address in dotted format notation, for example 201.10.8.1:<5080>. **Note 1:** If not specified, the REGISTER request is sent to the primary Proxy server (refer to 'Proxy IP address' parameter). **Note 2:** When port number is specified, DNS NAPTR/SRV queries aren't performed, even if ProxyDNSQueryType is set to 1 or 2.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 25 to 34)

ini File [Web Interface] Parameter Name	Description
TrunkGroupSettings [Hunt Group Settings]	(**Modification:** Added Registration Mode column.) Defines rules for port allocation for specific Hunt Groups. If no rule exists, the global rule defined by ChannelSelectMode applies. TrunkGroupSettings = <Hunt group ID>, <Channel select Mode>, <Registration Mode> The format is: a, b, c Where, a = Hunt Group ID number b = Channel select mode for that Hunt Group. c = Registration mode for that Hunt Group (Per Endpoint [0] or Per Hunt Group [1]). If not configured [-1], the value of AuthenticationMode is used. For example: TrunkGroupSettings = 1,5 **Note:** This parameter can appear up to 24 times.
CDRReportLevel [CDR Report Level]	(**Modification:** Additional enumeration 3.) Valid options include: ▪ 0 (None) = Call Detail Recording (CDR) information isn't sent to the Syslog server (default). ▪ 1 (End Call) = CDR information is sent to the Syslog server at end of each Call. ▪ 2 (Start & End Call) = CDR information is sent to the Syslog server at the start and at the end of each Call. ▪ 3 = CDR report is sent to Syslog at connection and at the end of each call. The CDR Syslog message complies with RFC 3161 and is identified by: Facility = 17 (local1) and Severity = 6 (Informational). **Note:** This parameter replaces the EnableCDR parameter.
StutterToneDuration [Stutter Tone Duration]	(**Modification:** Added support for Call Forwarding.) Duration (in msec) of the played Stutter dial tone, which indicates that Call Forwarding is enabled or that there is a waiting message(s). The default is 2,000 (i.e., 2 seconds). The range is 1,000 to 60,000. The Stutter tone is played (instead of a regular Dial tone), when a Call Forward is enabled on the specific port or when MWI is received. The tone is composed of a 'Confirmation tone', which is played for a user-defined duration (StutterToneDuration), followed by a 'Stutter tone'. Both tones are defined in the CPT file. **Note 1:** This parameter is applicable only to FXS gateways. **Note 2:** The message waiting notification (MWI) tone takes precedence over the call forwarding reminder tone.

1.8 Obsolete Parameters

Table 1-3 lists parameters from the previous release that are no longer in use.

Table 1-3: Release 5.0 Obsolete *ini* File [Web] Parameters

ini File [Web Interface] Parameter Name	Description
EnableProxySRVQuery	This parameter is obsolete; use instead the parameter ProxyDNSQueryType.
EnableSRVQuery	This parameter is obsolete; use instead the parameter DNSQueryType.
RTPNoOpEnable	This parameter is obsolete; use instead the parameter NoOperationSendingMode.
RTPNoOpInterval	This parameter is obsolete; use instead the parameter NoOpInterval.
IsHookFlashUsed	This parameter is obsolete; use instead the parameter HookFlashOption.

Reader's Notes

2 SIP Compatibility

2.1 Supported SIP Features

The MediaPack SIP main features are:

- Reliable User Datagram Protocol (UDP) transport, with retransmissions.
- Transmission Control Protocol (TCP) Transport layer.
- SIPS using TLS.
- T.38 real time Fax (using SIP).
  Note: If the remote side includes the fax maximum rate parameter in the SDP body of the INVITE message, the gateway returns the same rate in the response SDP.
- Works with Proxy or without Proxy, using an internal routing table.
- Fallback to internal routing table if Proxy is not responding.
- Supports up to four Proxy servers. If the primary Proxy fails, the gateway automatically switches to a redundant Proxy.
- Supports domain name resolving using DNS NAPTR and SRV records for Proxy, Registrar and domain names that appear in the Contact and Record-Route headers.
- Supports Load Balancing over Proxy servers using Round Robin or Random Weights.
- Proxy or Registrar Registration, such as:

```
REGISTER sip:servername SIP/2.0
VIA: SIP/2.0/UDP 212.179.22.229;branch=z9hG4bRaC7AU234
From: <sip:GWRegistrationName@sipgatewayname>;tag=1c29347
To: <sip:GWRegistrationName@sipgatewayname>
Call-ID: 10453@212.179.22.229
Seq: 1 REGISTER
Expires: 3600
Contact: sip:GWRegistrationName@212.179.22.229
Content-Length: 0
```

  - The "servername" string is defined according to the following rules:
  - The "servername" is equal to "RegistrarName" if configured. The "RegistrarName" can be any string.
  - Otherwise, the "servername" is equal to "RegistrarIP" (either FQDN or numerical IP address), if configured.
  - Otherwise the "servername" is equal to "ProxyName" if configured. The "ProxyName" can be any string.
  - Otherwise the "servername" is equal to "ProxyIP" (either FQDN or numerical IP address).

  The parameter GWRegistrationName can be any string. If the parameter is not defined, the parameter UserName is used instead.

The 'sipgatewayname' parameter (defined in the *ini* file or set from the Web browser), can be any string. Some Proxy servers require that the 'sipgatewayname' (in REGISTER messages) is set equal to the Registrar / Proxy IP address or to the Registrar / Proxy domain name.

The REGISTER message is sent to the Registrar's IP address (if configured) or to the Proxy's IP address. The message is sent per gateway or per gateway endpoint according to the "AuthenticationMode" parameter. Usually the FXS gateways are registered per gateway port, while FXO gateways send a single registration message, where Username is used instead of phone number in From/To headers. The registration request is resent according to the parameter 'RegistrartionTimeDivider'. For example, if 'RegistrationTimeDivider = 70' (%) and Registration Expires time = 3600, the gateway resends its registration request after 3600 x 70% = 2520 sec. The default value of 'RegistrartionTimeDivider' is 50%.

- Proxy and Registrar Authentication (handling 401 and 407 responses) using Basic or Digest methods. Accepted challenges are kept for future requests to reduce the network traffic.
- Single gateway Registration or multiple Registration of all gateway endpoints.
- Supported methods: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, INFO, REFER, UPDATE, NOTIFY, PRACK, SUBSCRIBE and PUBLISH.
- Modifying connection parameters for an already established call (re-INVITE).
- Working with Redirect server and handling 3xx responses.
- Early media (supporting 183 Session Progress).
- PRACK reliable provisional responses (RFC 3262).
- Call Hold and Transfer Supplementary services using REFER, Refer-To, Referred-By, Replaces and NOTIFY messages.
- Supports RFC 3711, Secured RTP and Key Exchange according to <draft-ietf-mmusic-sdescriptions-12>.
- Supports RFC 3489, Simple Traversal of UDP Through NATs (STUN).
- Supports RFC 3327, Adding 'Path' to Supported header.
- Supports RFC 3581, Symmetric Response Routing.
- Supports RFC 3605, RTCP Attribute in SDP.
- Supports RFC 3326, Reason header.
- Supports RFC 4028, Session Timers in SIP.
- Supports network asserted identity and privacy (RFC 3325 and RFC 3323).
- Support RFC 3911, The SIP Join Header.
- Support RFC 3903, SIP Extension for Event State Publication.
- Support RFC 3953, The Early Disposition Type for SIP.
- Support for RFC 3966, The tel URI for Telephone Numbers.
- Support RFC 4244, An Extension to SIP for Request History Information.
- Supports Tel URI (Uniform Resource Identifier) according to RFC 2806 bis.
- Supports ITU V.152 - Procedures for supporting Voice-Band Data over IP Networks.

- Remote party ID <draft-ietf-sip-privacy-04.txt>.
- Supports obtaining Proxy Domain Name(s) from DHCP (Dynamic Host Control Protocol) according to RFC 3361.
- Supports handling forking proxy multiple responses.
- RFC 2833 Relay for DTMF Digits, including payload type negotiation.
- DTMF out-of-band transfer using:
  - INFO method <draft-choudhuri-sip-info-digit-00.txt>
  - INFO method, compatible with Cisco gateways
  - NOTIFY method <draft-mahy-sipping-signaled-digits-01.txt>
- SIP URL: sip:"phone number"@IP address (such as 1225556@10.1.2.4, where "122556" is the phone number of the source or destination) or sip:"phone_number"@"domain name", such as 122556@myproxy.com. Note that the SIP URI host name can be configured differently per called number.
- Supports RFC 4040, RTP payload format for a 64 kbit/s transparent data.
- Can negotiate coder from a list of given coders.
- Supports negotiation of dynamic payload types.
- Supports multiple ptime values per coder.
- Supports RFC 3389, RTP Payload for Comfort Noise.
- Supports RFC 3824, Using E.164 numbers with SIP (ENUM).
- Supports reception and DNS resolution of FQDNs received in SDP.
- Supports <draft-ietf-sip-gruu-09>, Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP
- Responds to OPTIONS messages both outside a SIP dialog and in mid-call. Generates SIP OPTIONS messages as Proxy keep-alive mechanism.
- Publishes the total number of free Tel channels in a 200 OK response to an OPTIONS requests.
- Implementation of MWI IETF <draft-ietf-sipping-mwi-04.txt>, including SUBSCRIBE (to the MWI server). The MediaPack FXS gateways can accept an MWI NOTIFY message that indicates waiting messages or indicates that the MWI is cleared.
- Supports 3-Way Conference using an external media server.

2.2 Unsupported SIP Features

The following SIP features are NOT supported:

- MESSAGE method
- Preconditions (RFC 3312)
- SDP - Simple Capability Declaration (RFC 3407)
- S/MIME

2.3 SIP Compliance Tables

The MediaPack SIP gateways comply with RFC 3261, as shown in the following sections.

2.3.1 SIP Functions

Table 2-1: SIP Functions

Function	Supported
User Agent Client (UAC)	Yes
User Agent Server (UAS)	Yes
Proxy Server	Third-party only (tested with, amongst others, Ubiquity, Delta3, Microsoft, 3Com, Snom, and Cisco Proxies)
Redirect Server	Third-party
Registrar Server	Third-party
Event Publication Agent (EPA)	Yes
Event State Compositor (ESC)	Third-party

2.3.2 SIP Methods

Table 2-2: SIP Methods

Method	Supported	Comments
INVITE	Yes	
ACK	Yes	
BYE	Yes	
CANCEL	Yes	
REGISTER	Yes	Send only
REFER	Yes	
NOTIFY	Yes	
INFO	Yes	
OPTIONS	Yes	
PRACK	Yes	
UPDATE	Yes	
PUBLISH	Yes	Send only
SUBSCRIBE	Yes	

2.3.3 SIP Headers

The following SIP Headers are supported by the MediaPack SIP gateway:

Table 2-3: SIP Headers (continues on pages 40 to 42)

Header Field	Supported
Accept	Yes
Accept–Encoding	Yes
Alert-Info	Yes

Table 2-3: SIP Headers (continues on pages 40 to 42)

Header Field	Supported
Allow	Yes
Also	Yes
Asserted-Identity	Yes
Authorization	Yes
Call-ID	Yes
Call-Info	Yes
Contact	Yes
Content-Disposition	Yes
Content-Encoding	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Diversion	Yes
Encryption	No
Expires	Yes
Fax	Yes
From	Yes
History-Info	Yes
Join	Yes
Max-Forwards	Yes
Messages-Waiting	Yes
MIN-SE	Yes
Organization	No
P-Asserted-Identity	Yes
P-Preferred-Identity	Yes
Priority	No
Proxy- Authenticate	Yes
Proxy- Authorization	Yes
Proxy- Require	Yes
Prack	Yes
Record- Route	Yes
Refer-To	Yes
Referred-By	Yes
Replaces	Yes
Require	Yes
Remote-Party-ID	Yes
Response- Key	Yes
Retry- After	Yes
Route	Yes
Rseq	Yes
Session-Expires	Yes
Server	Yes
SIP-If-Match	Yes
Subject	Yes
Supported	Yes

Table 2-3: SIP Headers (continues on pages 40 to 42)

Header Field	Supported
Timestamp	Yes
To	Yes
Unsupported	Yes
User- Agent	Yes
Via	Yes
Voicemail	Yes
Warning	Yes
WWW- Authenticate	Yes

2.3.4 SDP Headers

The following SDP Headers are supported by the MediaPack SIP gateway:

Table 2-4: SDP Headers

SDP Header Element	Supported
v - Protocol version	Yes
o - Owner/ creator and session identifier	Yes
a - Attribute information	Yes
c - Connection information	Yes
d - Digit	Yes
m - Media name and transport address	Yes
s - Session information	Yes
t - Time alive header	Yes
b - Bandwidth header	Yes
u - Uri Description Header	Yes
e - Email Address header	Yes
i - Session Info Header	Yes
p - Phone number header	Yes
y - Year	Yes

2.3.5 SIP Responses

The following SIP responses are supported by the MediaPack SIP gateway:

- 1xx Response - Information Responses.
- 2xx Response - Successful Responses.
- 3xx Response - Redirection Responses.
- 4xx Response - Client Failure Responses.
- 5xx Response - Server Failure Responses.
- 6xx Response - Global Responses.

2.3.5.1 1xx Response – Information Responses

Table 2-5: 1xx SIP Responses

1xx Response		Supported	Comments
100	Trying	Yes	The SIP gateway generates this response immediately after receiving an INVITE request.
180	Ringing	Yes	The SIP gateway generates this response for an incoming INVITE message. On receiving this response, the gateway waits for a 200 OK response.
181	Call is being forwarded	Yes	The SIP gateway does not generate these responses. However, the gateway does receive them. The gateway processes these responses the same way that it processes the 100 Trying response.
182	Queued	Yes	The SIP gateway generates this response in Call Waiting service. When SIP gateway receives 182 response, it plays a special waiting Ringback tone to Tel side.
183	Session Progress	Yes	The SIP gateway generates this response if Early Media feature is enabled and if the gateway plays a Ringback tone to IP

2.3.5.2 2xx Response – Successful Responses

Table 2-6: 2xx SIP Responses

2xx Response		Supported	Comments
200	OK	Yes	
202	Accepted	Yes	

2.3.5.3 3xx Response – Redirection Responses

Table 2-7: 3xx SIP Responses

3xx Response		Supported	Comments
300	Multiple Choice	Yes	The gateway responds with an ACK and resends the request to first in the contact list, new address.
301	Moved Permanently	Yes	The gateway responds with an ACK and resends the request to new address.
302	Moved Temporarily	Yes	The SIP gateway generates this response when call forward is used, to redirect the call to another destination. If such response is received, the calling gateway initiates an INVITE message to the new destination.
305	Use Proxy	Yes	The gateway responds with an ACK and resends the request to new address.
380	Alternate Service	Yes	"

2.3.5.4 4xx Response – Client Failure Responses

Table 2-8: 4xx SIP Responses (continues on pages 44 to 45)

4xx Response		Supported	Comments
400	Bad Request	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
401	Unauthorized	Yes	Authentication support for Basic and Digest. On receiving this message the GW issues a new request according to the scheme received on this response
402	Payment Required	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
403	Forbidden	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
404	Not Found	Yes	The SIP gateway generates this response if it is unable to locate the callee. On receiving this response, the gateway notifies the User with a Reorder Tone.
405	Method Not Allowed	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
406	Not Acceptable	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
407	Proxy Authentication Required	Yes	Authentication support for Basic and Digest. On receiving this message the GW issues a new request according to the scheme received on this response.
408	Request Timeout	Yes	The gateway generates this response if no-answer timeout expired. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
409	Conflict	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
410	Gone	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
411	Length Required	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
413	Request Entity Too Large	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
414	Request-URL Too Long	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
415	Unsupported Media	Yes	If the gateway receives a 415 Unsupported Media response, it notifies the User with a Reorder Tone. The gateway generates this response in case of SDP mismatch.
420	Bad Extension	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.

Table 2-8: 4xx SIP Responses (continues on pages 44 to 45)

4xx Response		Supported	Comments
480	Temporarily Unavailable	Yes	If the gateway receives a 480 Temporarily Unavailable response, it notifies the User with a Reorder Tone. This response is issued if there is no response from remote.
481	Call Leg/Transaction Does Not Exist	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
482	Loop Detected	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
483	Too Many Hops	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
484	Address Incomplete	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
485	Ambiguous	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
486	Busy Here	Yes	The SIP gateway generates this response if the called party is off hook and the call cannot be presented as a call waiting call. On receiving this response, the gateway notifies the User and generates a busy tone.
487	Request Canceled	Yes	This response indicates that the initial request is terminated with a BYE or CANCEL request.
488	Not Acceptable	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.

2.3.5.5 5xx Response – Server Failure Responses

Table 2-9: 5xx SIP Responses

5xx Response		Comments
500	Internal Server Error	On reception of any of these Responses, the GW releases the call, sending appropriate release cause to PSTN side. The GW generates 5xx response according to PSTN release cause coming from PSTN.
501	Not Implemented	
502	Bad gateway	
503	Service Unavailable	
504	Gateway Timeout	
505	Version Not Supported	

2.3.5.6 6xx Response – Global Responses

Table 2-10: 6xx SIP Responses

6XX Response		Comments
600	Busy Everywhere	On reception of any of these Responses, the GW releases the call, sending appropriate release cause to PSTN side.
603	Decline	
604	Does Not Exist Anywhere	
606	Not Acceptable	

3 Known Constraints

3.1 Hardware Constraints

1. Only specific combinations of FXS and FXO modules are currently supported. For detailed information, contact AudioCodes.
2. MP-11x - After running the procedure for restoring the networking parameters to their initial state, the gateway must be reset again using a hardware reset. If a software reset is issued, the gateway reverts to its factory defaults.

3.2 SIP Constraints

1. The 'Netcoder' coder is no longer supported.
2. The number of RTP payloads packed in a single G.729 packet (M channel parameter) is limited to 5.
3. The STUN protocol is used only when the transport protocol is UDP. STUN doesn't support TCP. In addition, STUN doesn't function when the gateway is behind a Symmetric NAT.
4. If the gateway is not configured to use RFC 2833 for Hook-Flash and the remote side sends such a signal, it is disregarded. In addition, if the gateway initiates the SIP INVITE with RFC 2833 supported and the remote side does not support this method, the gateway still generates the Hook-Flash signal.

3.3 Gateway Constraints

1. The device attempts to access the incorrect TFTP server when IniFileUrl specifies a TFTP URL. It is possible to work-around this problem by resetting the device (using the Web interface) after the TFTP error occurs.
2. RFC 2198 redundancy mode with RFC 2833 is not supported (that is, if a complete DTMF digit was lost, it is not reconstructed). The current RFC 2833 implementation does support redundancy for inter-digit information lost.
3. Date and Time should be set after each gateway power reset, unless NTP (Network Time Protocol) is used.
4. After resetting the Web password using the *ini* file parameter ResetWebPassword and defining a new password, the user must load an *ini* file with ResetWebPassword set to 0.
5. Channel parameters, such as, Voice/DTMF gain and Jitter buffer are collectively configured in the *ini* file on a per gateway usage (not on a per call basis). By using Profiles this limitation can be overcome.
6. The gateway only supports symmetrical coders – the same coder is used for transmit and for receive (though different ptime is supported).

7. The following constraints apply when defining coders via the *ini* file.
   - Coder names are case-sensitive.
   - Don't use obsolete coder names (e.g., g729_AnnexB, g7231r53) with the improved coder interface.
   - When an invalid packetization time is used, the coder definition is disregarded.
   - When an invalid rate is used for dynamic-rate coders, the coder definition is disregarded.
8. The 'RFC2833RxPayloadType' and 'RFC2833TxPayloadType' parameters in the Embedded Web Server's 'Channel Settings' screen or in the *ini* file should not be used. Use the parameter 'Rfc2833PayloadType' instead.
9. Configuring the board to auto-negotiate mode while the opposite port is set manually to full-duplex (either 10 Base-T or 100 Base-TX) is invalid. It is also invalid to set the board to one of the manual modes while the opposite port is configured differently. It is recommended to use full-duplex connections instead of half-duplex, and 100 Base-TX instead of 10 Base-T (due to the larger bandwidth).
10. It is strongly recommended to use 100 Base-T switches. Use of 10 Base-T LAN hubs should be avoided.
11. In some cases, when the spanning tree algorithm is enabled on the external Ethernet switch port connected to the gateway, the external switch blocks traffic entering and exiting the gateway for some time after the gateway is reset. This may cause the loss of important packets (such as BootP and TFTP requests) which in turn may cause the board to fail to start up. A possible workaround for this issue is to set the parameter BootPRetries to 5, forcing the gateway to issue 20 BootP requests for 60 seconds. A second workaround is to disable the spanning tree algorithm on the port of the external switch that is connected to the gateway.
12. When RTP packets are received after a sudden large network delay (200 to 300 msec), the drift correction could take about 5 seconds. During this period, voice towards the TDM side is silent.
13. Static NAT is not supported for local IP calls.
14. MP-118 FXO: NTT Ring Detection is not supported (with or without caller ID).
15. MP-118 FXO: Indian Caller ID detection is not supported.
16. MP-118 FXO: Metering tone (billing) detection is currently not supported.
17. VLAN Pass-Through mode is not supported.
18. NTT caller ID type two constraints:
    - The NTT standard describes the CallerID type 2 generation as a sequence of an incoming-call signal, 'C' & 'D' DTMFs and FSK modulated data. Generation of the incoming call signal remains in the responsibility of the application, but 'C', 'D' and the FSK are generated by the supplied service. The signal can be generated using the UDT signal generation mechanism.
    - Prior to the detection of NTT CallerID type 2 there are 2 DTMF ('C' and 'D') detections which remain unscreened.
19. MP-124 rev A and MP-124 rev B do not support the following:
    - Long haul
    - Caller ID generation
    - MWI generation

20. The level field in the detection event of burst tone should be ignored (is always equal to -63 dBm).
21. Setting the V.21 Transport Type to Bypass and Fax Transport Type to relay results in entering Fax Relay mode at the 2100 Hz signal. Only at the end of this signal, does the channel enter Bypass mode.
22. If PCM LoopBack is activated, there is no way of knowing if a new channel being opened is in LoopBack state or not. The parameter should only be used for test-purposes.
23. When using FaxTransportType = TransparentWithEvents, the Fax events parameters regarding the side of the fax call (answering or calling) and the number of pages are invalid.
24. The number of channels operating in internal IP loopback mode that can be supported by the board is usually less than the declared channel capacity.
25. The resolution of the duration of digits On and Off time when dialing to the network using RFC 2833 relay, is dependent on the basic frame size of the coder being used.
26. Flash-burning control for specific files (BurnCASFile, BurnCallProgressToneFile, BurnVXMLFile, BurnVoicePromptsFile) is no longer supported. Everything is now controlled by the new parameter SaveConfiguration

3.4 Web Constraints

1. The AGC parameters in the 'Channel Settings' screen are not applicable to the gateway.
2. Incorrect presentation of dynamic payload in the 'Channel Status' screen.
3. The 'Fax/Modem Bypass Packing Factor' field doesn't support the 'G726_32' and 'G726_40' options.
4. After resetting the Web password using the *ini* file parameter ResetWebPassword and defining a new password, the user must load an *ini* file with ResetWebPassword set to 0.
5. The Embedded Web Server cannot be accessed with HTTPS when DES/3DES is selected on Microsoft Internet Explorer. If the gateway is configured to use the DES cipher, a logic error in Microsoft Internet Explorer causes the HTTPS connection to fail. This problem does not occur when using alternative browsers, such as Firefox.
6. Username and password with 8 characters cannot be entered.
7. Not all parameters can be changed on-the-fly from the Web browser. Parameters that can't be changed on-the-fly are noted with (!). To change these parameters, reset the gateway, using the Web browser reset button.
8. When changing gateway parameters from the Web browser, the new parameters are permanently stored in flash memory only after the gateway is reset from the Web or after the **BURN** button is clicked in the 'Maintenance Actions' screen.
9. The number of fax calls indicated by the fields: 'Attempted Fax Calls Counter' and 'Successful Fax Calls Counter' in the Calls Count screens may not be accurate.
10. In the screens 'Coders' and 'Coder Group Settings': When G.729 is used with ptimes 80, 100 and 120 and G.723 is used with ptimes 120 and 150 the voice quality is reduced. Therefore, using these ptimes isn't recommended.

11. The 'Caller ID/Name' column in the 'Caller ID' table in the Embedded Web Server can't contain the inverted commas character ("). For example entering "John" is not allowed. In the *ini* file this string can be used.
12. Incorrect values are displayed on the "Firewall settings" Web page, after the firewall rules are manipulated, using SNMP. The problem only occurs when mixing management interfaces; i.e., working with the Web interface, then switching to SNMP, then switching back to the Web.
13. Can not access the device's Web interface using HTTPS using Microsoft™ Internet Explorer if DES/3DES is selected. If the device is configured to use the DES cipher, a logic error in Microsoft™ Internet Explorer would cause the HTTPS connection to fail. This problem does not occur when using alternative browsers, such as Firefox™.
14. An *ini* file with parameters in table format can not be sent to a board.
15. Logo and product name revert to default with an empty ini file.
16. When "Access to Restricted Domains" is set to ON, all attempts to enter security pages sends a Syslog message, apart from CERTIFICATES page (both Security/certificates and SSLCertificateSR pages).
17. Parameter values set commands that are sent to the Syslog. Values are shown which are offset from the values entered in the Web; e.g., when VoiceVolume is set to X, the Syslog message indicates the value X+32.
18. When configuring the RadiusAuthServerIp parameter with a non-existent server IP, the BehaviorUponRadiusTimeout parameter value is ignored.
19. Wrong presentation of dynamic payload in the channel status page.
20. The value of Fax Modem Bypass Coder Type in the Web is absent.
21. SNMPv3 users table returns "line removed" notice when adding a new row to an active row index.
22. Firefox/mozilla- Part of the port Info box of Ch 1-4 is obscured by the left menu.
23. After adding an empty line to SNMPV3 table it is impossible to delete it or add new lines.
24. Wizard gets stuck upon attempt to load an inappropriate file type.
25. Firefox/Mozilla: Port info text box opens too far away from the port.
26. Unintended password reset when changing the username and/or password via the Web and Reset board again from Web.
27. When performing a GET Complete ini file via the Web, swwd messages appear.

3.5 SNMP Constraints

1. An Ethernet link trap is sent before link is up; manager does not receive clear. This occurs because a spanning tree algorithm is being calculated in the Ethernet switch.
2. The acBoardConfigurationError alarm trap, generated as a result of a configuration error, does not clear.
3. The range of the faxModemRelayVolume MIB object is wrong. Instead of 0 to 15, it should be -18 to -3, corresponding to an actual volume of -18.5 dBm to -3.5 dBm.
4. Cold-start trap doesn't appear after soft reset for MediaPack.
5. Only one SNMP manager can access the device simultaneously.

6. The default values created in an IPSec configuration table are wrong. The user should override the default values before activating the new row.
7. Only one SNMP manager can access the boards/modules at one time.
8. The following RTP MIB objects are not supported:
   - rtpRcvrSRCSSRC
   - rtpRcvrSSRC
   - rtpSenderSSRC
   - rtpRcvrLostPackets
   - rtpRcvrPackets
   - rtpSenderPackets
   - rtpRcvrOctets
   - rtpSenderOctets
9. The following encryptions types are currently supported (for SNMP v3 users only):
   - Authentication protocol – MD5 and SHA
   - Privacy protocol – DES and AES128

Reader's Notes

4 Previous Release 4.8

4.1 Supported Hardware Platforms

4.1.1 New Hardware Platforms Introduced in This Release

The following hardware platforms are introduced in this version:

- MP-118/FXO with 8 FXO ports and MP-114/FXO with 4 FXO ports.
- MP-118/FXS + FXO with 4 FXS ports and 4 FXO ports. This gateway contains a relay that connects the FXS ports to the FXO ports in case of a power failure.
- MediaPack MP-124/FXS Rev D, 24 analog FXS interfaces.

4.1.2 Existing Hardware Platforms

- Analog Mediant 1000 hosting FXS or FXO modules (up to 4 ports in each module, with a total of 6 modules providing up to 24 ports).
- MediaPack MP-11x/FXS, 2 to 8 analog FXS interfaces, with enhanced CPU resources.
  - MediaPack MP-118/FXS, 8 analog FXS interfaces.
  - MediaPack MP-114/FXS, 4 analog FXS interfaces.
  - MediaPack MP-112/FXS, 2 analog FXS interfaces.

4.1.3 Hardware Platforms No Longer Supported

- MediaPack MP-108/FXS, 8 analog FXS interfaces
- MediaPack MP-108/FXO, 8 analog FXO interfaces
- MediaPack MP-104/FXS, 4 analog FXS interfaces
- MediaPack MP-104/FXO. 4 analog FXO interfaces
- MediaPack MP-102/FXS, 2 analog FXS interfaces
- MediaPack MP-124/FXS Rev A, B, C, 24 analog FXS interfaces.

4.2 General Gateway New Features

1. Support for the IPSec and IKE protocols was added. IPSec and IKE are part of the IETF standards for establishing a secured IP connection between two applications. Providing security services at the IP layer, IPSec and IKE are transparent to IP applications.
   IPSec and IKE are used in conjunction to provide security for control (e.g., SIP) and management (e.g., SNMP and Web) protocols but not for media (i.e., RTP, RTCP and T.38).
   Relevant Parameters: EnableIPSec and the following table parameters: IPSEC_IKEDB_TABLE, IPSEC_SPD_TABLE (for detailed information on the parameters of each table, refer to the User's Manual).

2. The following NAT traversal mechanisms were added:

   - The gateway now supports the Simple Traversal of UDP Through NATs (STUN) protocol according to RFC 3489. This mechanism enables the gateway to discover the presence (and types) of NATs and firewalls located between it and the public Internet. It also provides the gateway with the capability to determine the public IP address allocated to the NAT. This information is later embedded in outgoing SIP/SDP messages and enables remote SIP user agents to reach the gateway.
     Relevant parameters: EnableSTUN, STUNServerPrimaryIP, STUNServerSecondaryIP, NATBindingDefaultTimeout.
   - To enable NAT traversal for the RTP streams RTP NO-OP packets (according to avt-rtp-noop draft) are now sent. This method ensures that the NAT binding remains open during RTP silence periods.
     Relevant parameters: RTPNoOpEnable, RTPNoOpInterval, RTPNoOpPayloadType.
   - Can now configure the gateway to send keep alive traps to a different UDP port.
     Relevant parameter: KeepAliveTrapPort.

3. The interface for handling coders was improved. You can now select the coder family, packetization time, rate (where applicable), payload type (where applicable) and silence suppression individually per coder.
   Relevant parameters: CoderName, CoderName_ID.

4. Additional parameters were added to the IP and Tel Profiles. In addition, the number of different IP and Tel Profiles was increased to 10 each.
   Relevant parameters: IPProfile, TelProfile.

5. FXS gateways now support generation of 12/16 KHz metering pulses towards the Tel side (e.g., for connection to a payphone or private meter). Tariff pulse rate is determined according to an internal table. This capability enables users to define different tariffs according to the Source/Destination numbers and the time-of-day. The tariff includes the time interval between the generated pulses and the number of pulses generated on answer.
   Relevant parameters: ChargeCode, MeteringType, PayPhoneMeteringMode, Prefix.

6. The RADIUS Accounting mechanism is now supported. The gateway sends a CDR to the RADIUS Accounting Server at the start and/or end of each call.
   Relevant parameters: AAAIndications, RADIUSAccServerIP, RADIUSAccPort, RADIUSAccountingType.

7. FXO gateways can now disconnect a call after a dial tone from the PBX is detected. This is in addition to the existing capability of call disconnection when either busy or reorder tones are detected.
   Relevant parameters: DisconnectOnDialTone.

8. FXO gateways now support a 'guard' time between accepting successive IP to Tel calls. Occasionally, after a call is ended and onhook is applied, a delay is required before placing a new call (and performing offhook). This is necessary to prevent wrong hook-flash detection or other glare phenomena.
Relevant parameters: GuardTimeBetweenCalls.

9. FXS gateways can now add a delay between detection of offhook and generation of DID Wink.
Relevant parameters: DelayBeforeDIDWink.

10. It is now possible to determine the behavior of FXS endpoints that are not defined (in the Endpoint Phone Number table), and the behavior of all FXS endpoints when a Busy-Out condition exists. Up to this version, the gateway played a reorder tone to the connected phone/PBX. It is now possible to set the behavior of such endpoints to either no response, reorder tone, polarity reversal, or both.
Relevant parameters: FXSOOSBehavior.

11. It is now possible to define a digit pattern that is sent to the Tel side after 200 OK is received from the IP side. The digit pattern is a predefined DTMF sequence that is used to indicate an answer signal (e.g., for billing purposes). Applicable only to FXS gateways.
Relevant parameters: TelConnectCode.

12. The parameter 'Source Number before Manipulation' was added to CDR messages.

13. The MediaPack can now be configured to set a different DiffServ value to IP packets according to their class-of-service (Network, Premium Media, Premium Control, Gold and Bronze).
Relevant Parameters: NetworkServiceClassDiffServ, PremiumServiceClassMediaDiffServ, PremiumServiceClassControlDiffServ, GoldServiceClassDiffServ, BronzeServiceClassDiffServ.

14. Life line testing – The MediaPack now features a mechanism that performs tests on the telephone lines connected to FXS and FXO ports. These tests provide various line measurements. Line testing is executed via SNMP only.

15. Full Mesh Routing – The MediaPack now supports a combination of FXS and FXO channels (4 FXS and 4 FXO channels). Each FXS channel features a lifeline that is connected to a FXO channel [channel 1 (FXS) to channel 5 (FXO)], [channel 2 (FXS) to channel 6 (FXO)] and so on.
Relevant parameter: LifeLineType.

16. IP Multicast – Supports the reception of multicast RTP streams. The gateway can join an IP multicast group in order to receive an RTP stream generated by a remote server (e.g., a Music-On-Hold stream) to a multicast IP address.

17. PPPoE – The MediaPack can now operate as a Point-to-Point Protocol over Ethernet (PPPoE) client, enabling it to be integrated in a broadband access architecture (mostly in ISP networks).
Relevant parameters: EnablePPPoE; PPPoEPassword; PPPoERecoverIPAddress; PPPoERecoverDfgwAddress; PPPoERecoverSubnetMask; PPPoEServerName; PPPoEStaticIPAddress; PPPoEUserName.

18. The Multiple IPs mechanism can now support a dual mode, separating the Media from the OAM and Control networks.

19. Internal firewall – The MediaPack now accommodates an internal access list facility, allowing the security administrator to define network traffic filtering rules.
Relevant table parameter: AccessList.

20. Up to five simultaneous Telnet sessions are now supported.

21. Support for DTMF relay according to RFC 2833 was added to the ThroughPacket™ mechanism.

22. An Activity Log mechanism was added to enable the MediaPack to send log messages (to a Syslog server) that report certain types of web actions according to a pre-defined filter.
The following filters are available: Parameters Value Change, Auxiliary Files Loading, Device Reset, Flash Memory Burning, Device Software Update, Access to Restricted Domains, Non Authorized Access and Sensitive Parameters Value Change.
Relevant parameter: ActivityListToLog.

23. The automatic update mechanism enables loading files also via FTP, FTPS and Network File System (NFS).

24. Initial configuration of the gateway can now be performed using a standard touch-tone telephone connected to one of the FXS analog ports. The voice menu can also be used to query and modify basic configuration parameters.
Relevant parameter: VoiceMenuPassword.

25. As of this version it isn't required to load a coefficients file to FXO gateways; instead there is a single parameter that defines the country variant (doesn't apply to the Mediant 1000).
Relevant parameter: CountryCoefficients.

4.3 SIP New Features

1. MediaPack only. The gateway now supports Secured RTP (SRTP) according to RFC 3711. SRTP is used to encrypt RTP and RTCP transport. SRTP requires a Key Exchange mechanism that is performed according to <draft-ietf-mmusic-sdescriptions-12>. The Key Exchange is executed by adding a 'Crypto' attribute to the SDP. This header is used (by both sides) to declare the various supported cipher suites and to attach the encryption key to use. If negotiation of the encryption data is successful, the call is established.
Use of SRTP may reduce the number of available channels.
Relevant parameters: EnableMediaSecurity, MediaSecurityBehaviour.

2. Support was added for hunt group usage and declaration according to <draft-ietf-iptel-trunk-group-04>. If enabled, the hunt group number is added as the 'tgrp' parameter to the Contact header of outgoing SIP messages. For incoming SIP messages, if the Request-URI includes a 'tgrp' parameter, the gateway routes the call according to that value (if possible). In addition, if the incoming Contact header contains a 'tgrp' parameter, it is copied to the corresponding outgoing messages in that dialog.
Relevant parameters: UseSIPTgrp.

3. A new auxiliary file (User Information) was added. This file contains a list of PBX extensions and their attributes (i.e., global phone number, display name, user name and password). This information is loaded to the gateway and is used to emulate a large number of SIP user agents. Each entry (defined by the User Information file) is registered separately, emulating the behavior of an IP phone.
This file can be loaded via the *ini* file, the Embedded Web Server or by using the automatic update mechanism.
Relevant parameters: EnableUserInfoUsage, UserInfoFileName, UserInfoFileURL.

4. It is now possible to configure the string that is used in the SIP request header 'User-Agent' and SIP response header 'Server'.
Relevant parameters: UserAgentDisplayInfo.

5. It is now possible to select the SIP method used for session-timer updates. Two options are available: the currently supported re-INVITE request and the new request UPDATE. The gateway can receive session-timer refreshes using both methods. Relevant parameters: SessionExpiresMethod.

6. The Proxy Keep-Alive mechanism can now use REGISTER messages instead of OPTIONS messages. Any response received from the Proxy, either success (200 OK) or failure (a 4xx response) is considered as if the Proxy is communicating. Relevant parameters: EnableProxyKeepAlive.

7. The gateway now supports dynamic Payload Type (PT) negotiation for the relevant coders. For IP to Tel calls, if an incoming INVITE includes a coder that uses a dynamic PT, the gateway uses the PT defined by the remote side and ignores its configuration. For Tel to IP calls, the gateway sets the dynamic PT in the SDP according to its configuration but uses the PT defined by the remote side.

8. The gateway now supports reception and DNS resolution of Fully Qualified Domain Names (FQDNs) received in SDP.

9. The authentication process was improved in order to reduce the number of SIP messages transmitted on the network. The very first request to the active Proxy is sent without authorization. The Proxy sends a 401/407 response with a challenge. This response is saved for further uses. A new request is resent with the appropriate credentials. Following requests to the active Proxy are sent with credentials (calculated from the saved challenge). If the Proxy doesn't accept the new request and sends another challenge, the old challenge is replaced with the new one.

10. It is now possible to configure the value assigned to the Subject header. If configured, the Subject header is added to all outgoing INVITE messages. Relevant parameters: SIPSubject.

11. The DTMF transport mechanism was improved. You can now set the preferred DTMF transport methods according to priority. In addition, the number of configuration parameters was reduced. Relevant parameters: TxDTMFOption.

12. Handling of the OPTIONS method was improved:

    - If an OPTIONS message is received without a user in the Request-URI, a 200 OK response is sent.
    - If an OPTIONS message is received with a user in the Request-URI, the gateway tries to find a corresponding user endpoint. If no endpoint is found, the gateway responds with 404 Not Found. If an endpoint is found but this endpoint is currently busy, the gateway responds with 486 Busy Here. If an endpoint is found and it is free, the gateway responds with 200 OK.
    - If the gateway responds with 200 OK, it always includes an SDP body (that includes all supported coders) in the response, in addition, it fills the Supported header with the supported capabilities and the Require header if 100rel (PRACK) is required by the configuration.

13. The number of total and free channels was added to a 200 OK response to an OPTIONS request. The gateway uses the X-Resource header in the following format: 'X-Resource: telchs=5/8;mediachs=0/0'. Where 'telchs' specifies the number of free tel channels / total tel channels. The parameter 'mediachs' should be ignored.

14. It is now possible to determine the format of the URI in the P-Asserted and P-Preferred headers.

    Relevant parameters: UseTelURIForAssertedID.

15. It is now possible to indicate that a call is waiting using 180 Ringing response (instead of 182).

    Relevant parameters: Send180ForCallWaiting.

16. It is now possible to configure the gateway's behavior in response to 3xx messages. The redirected INVITE can either use the same call identifiers (*CallID*, *branch*, *to* and *from* tags) or modify these identifiers as a new call. Relevant Parameters: 3xxBehavior.

4.4 Web and SNMP New Features

1. To prevent unauthorized access to the Embedded Web Server, two user accounts are now available, a primary and secondary. Each account is composed of three attributes: username, password and access level. The username and password enable access to the Embedded Web Server itself; the access level determines the extent of the access (i.e., availability of screens and read / write privileges). Relevant parameter: ResetWebPassword.
2. SNMP community strings can now be configured via the Embedded Web Server. Relevant parameters: SNMPReadOnlyCommunityString_x, SNMPReadWriteCommunityString_x, SNMPTrapCommunityString.
3. A new channel status screen provides the status of the R factor of RTCP XR packets per channel.
4. The Mediant 1000 chassis can now be managed via SNMP. The status of the CPU and I/O modules, fan tray, power supplies, Power Entry Module (PEM) and other alarms are reported.
5. An HTTP download report trap is now available. This trap indicates the result of a recent file download (includes an HTTP error code, if available).
6. Support for 'sysObjectID' via SNMP was added. Similar to MIB-Object's definition. Should point to a product that is defined in AC-TYPES.my.
7. Active analog lines performance counter is now supported in analog performance monitoring.

4.5 Resolved Constraints

The gateway now responds to OPTIONS messages received in mid-call (during a SIP dialog).

4.6 New and Modified Parameters

Most new parameters (described in Table 4-1) can be configured with the *ini* file and via the Embedded Web Server. Note that only those parameters contained within square brackets are configurable via the Embedded Web Server.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

***ini* File [Web Interface] Parameter Name**	**Description**
EnableIPSec [Enable IP Security]	Enables / disables the Secure Internet Protocol (IPSec) on the gateway. 0 = Disable (default). 1 = Enable.
EnableSTUN [Enable STUN]	0 = STUN protocol is disabled (default). 1 = STUN protocol is enabled. When enabled, the gateway functions as a STUN client and communicates with a STUN server located in the public internet. STUN is used to discover whether the gateway is located behind a NAT and the type of that NAT. In addition, it is used to determine the IP addresses and port numbers that the NAT assigns to outgoing signaling messages (using SIP) and media streams (using RTP, RTCP and T.38). STUN works with many existing NAT types, and does not require any special behavior from them. This parameter cannot be changed on-the-fly and requires a gateway reset.
STUNServerPrimaryIP [STUN Server Primary IP]	The IP address of the primary STUN server.
STUNServerSecondaryIP [STUN Server Secondary IP]	The IP address of the secondary STUN server.
NATBindingDefaultTimeout	Defines the default NAT binding lifetime in seconds. STUN is used to refresh the binding information after this time expires. The valid range is 0 to 2592000. The default value is 30.
RTPNoOpEnable	Enables / disables sending of NO-OP packets. 0 = Disabled (default). 1 = Enabled. This mechanism ensures that the NAT binding remains open during RTP silence periods.
RTPNoOpInterval	Determines the time interval (in msec) in which NO-OP packets is sent in the case of silence (no RTP traffic). The valid range is 20 to 600000. The default value is 1000 (10 seconds).
RTPNoOpPayloadType	Determines the payload type of No-Op packets. The valid range is 96 to 127. The default value is 120.
UseSIPTgrp [Use Tgrp Information]	0 = Tgrp parameter isn't used (default). 1 = (send only) The hunt group number is added as the 'tgrp' parameter to the Contact header of outgoing SIP messages. If a hunt group number is not associated with the call, the 'tgrp' parameter isn't included. If a 'tgrp' value is specified in incoming messages, it is ignored. 2 = (send and receive) The functionality of outgoing SIP messages is identical to the functionality described in option (1). In addition, for incoming SIP messages, if the Request-URI includes a 'tgrp' parameter, the gateway routes the call according to that value (if possible). If the Contact header includes a 'tgrp' parameter, it is copied to the corresponding outgoing messages in that dialog.
UserAgentDisplayInfo [User-Agent Information]	Defines the string that is used in the SIP request header 'User-Agent' and SIP response header 'Server'. If not configured, the default string 'AudioCodes product-name s/w-version' is used (e.g., User-Agent: Audiocodes-Sip-Gateway-MP-118 FXS/v.4.80.004.008). When configured, the string 'UserAgentDisplayInfo s/w-version' is used (e.g., User-Agent: MyNewOEM/v.4.80.004.008). Note that the version number can't be modified. The maximum string length is 50 characters.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

***ini* File [Web Interface] Parameter Name**	**Description**
SessionExpiresMethod [Session Expires Method]	Defines the SIP method used for session-timer updates. 0 = Use Re-INVITE messages for session-timer updates (default). 1 = Use UPDATE messages. **Note:** The gateway can receive session-timer refreshes using both methods.
IPProfile_ID [IP Profile Settings]	IPProfile_<Profile ID> = <Profile Name>,<Preference>,<Coder Group ID>,<IsFaxUsed *>,<DJBufMinDelay *>, <DJBufOptFactor *>,<IpDiffServ *>,<ControlIPDiffServ *>,<N/A use $$ instead>, <RTPRedundancyDepth>, <RemoteBaseUDPPort>, <CNGmode>, <VxxTransportType>, <NSEMode>, <PlayRBTone2IP>, <EnableEarlyMedia*>, <ProgressIndicator2IP*> Preference = (1-20) The preference option is used to determine the priority of the Profile. Where '20' is the highest preference value. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied. For example: IPProfile_1 = name1,2,1,0,10,13,15,44,1,1,6000,0,2,0,0,1,0 IPProfile_2 = name2,$$,$$,$$,$$,$$,$$,$$,$$,1,$$,$$,$$,$$,$$,$$,$$ $$ = Not configured, the default value of the parameter is used. (*) = Common parameter used in both IP and Tel profiles. **Note 1:** The IP ProfileID can be used in the Tel2IP and IP2Tel routing tables (Prefix and PSTNPrefix parameters). **Note 2:** 'Profile Name' assigned to a ProfileID, enabling User's to identify it intuitively and easily. **Note 3:** This parameter can appear up to 9 times (ID = 1 to 9).
TelProfile_ID [Tel Profile Settings]	TelProfile_<Profile ID> = <Profile Name>,<Preference>,<Coder Group ID>,<IsFaxUsed *>,<DJBufMinDelay *>, <DJBufOptFactor *>,<IPDiffServ *>,<ControlIPDiffServ*>,<DtmfVolume>,<InputGain>, <VoiceVolume>,<EnableReversePolarity>,<EnableCurrentDisconnect>, <EnableDigitDelivery>, <ECE>, <MWIAnalogLamp>, <MWIDisplay>, <FlashHookPeriod>, <EnableEarlyMedia*>, <ProgressIndicator2IP*> Preference = (1-20) The preference option is used to determine the priority of the Profile. Where '20' is the highest preference value. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied. For examples: TelProfile_1 = FaxProfile,1,1,1,40,13,22,33,$$,$$,$$,0,0,0,1,0,0,$$,0,$$ TelProfile_2 = ModemProfile,2,2,0,40,13,$$,$$,$$,$$,$$,$$,$$,$$,0,0,0,$$,0,$$ $$ = Not configured, the default value of the parameter is used. (*) = Common parameter used in both IP and Tel profiles. **Note 1:** The Tel ProfileID can be used in the Hunt group table (TrunkGroup_x parameter). **Note 2:** 'Profile Name' assigned to a ProfileID, enabling User's to identify it intuitively and easily. **Note 3:** This parameter can appear up to 9 times (ID = 1 to 9).

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

***ini* File [Web Interface] Parameter Name**	**Description**
EnableProxyKeepAlive [Enable Proxy Keep Alive]	0 = Disable (default). 1 = Enable Keep alive with Proxy using OPTIONS. 2 = Enable Keep alive with Proxy using REGISTER. If EnableProxyKeepAlive = 1, SIP OPTIONS message is sent every ProxyKeepAliveTime. If EnableProxyKeepAlive = 2, SIP REGISTER message is sent every RegistrationTime. Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is correctly communicating. **Note 1:** This parameter must be set to 1 (OPTIONS) when Proxy redundancy is used. **Note 2:** When EnableProxyKeepAlive = 2 (REGISTER), the homing redundancy mode is disabled.
ProxyKeepAliveTime [Proxy Keep Alive Time]	Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages. The default value is 60 seconds. **Note:** This parameter is applicable only if EnableProxyKeepAlive = 1 (OPTIONS). When EnableProxyKeepAlive = 2 (REGISTER), the time interval between Keep-Alive messages is determined by the parameter RegistrationTime.
[RegistrationTime] Registration Time	Defines the time (in seconds) for which registration to a Proxy server is valid. The value is used in the header 'Expires'. In addition, this parameter defines the time interval between Keep-Alive messages when EnableProxyKeepAlive = 2 (REGISTER). Typically, a value of 3600 should be assigned for one hour registration. The gateway resumes registration according to the parameter RegistrationTimeDivider. The default is 180 seconds.
UseTelURIForAssertedID	Determines the format of the URI in the P-Asserted and P-Preferred headers. 0 = 'sip:' (default). 1 = 'tel:'.
UseSourceNumberAsDisplayName [Use Source Number as Display Name]	Applicable to Tel→IP calls. 0 = No. The Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name (if Tel Display Name is received). If no Display Name is received from the Tel side, the IP Display Name remains empty (default). 1 = Yes. If a Tel Display Name is received, the Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name. If no Display Name is received from the Tel side, the Tel Source Number is used as the IP Source Number and also as the IP Display Name. 2 = Overwrite. The Tel Source Number is used as the IP Source Number and also as the IP Display Name (even if the received Tel Display Name is not empty).
UseDisplayNameAsSourceNumber [Use Display Name as Source Number]	Applicable to IP→Tel calls. 0 = No. The IP Source Number is used as the Tel Source Number and the IP Display Name is used as the Tel Display Name (if IP Display Name is received). If no Display Name is received from IP, the Tel Display Name remains empty (default). 1 = Yes. If an IP Display Name is received, it is used as the Tel Source Number and also as the Tel Display Name, the Presentation is set to Allowed (0). If no Display Name is received from IP, the IP Source Number is used as the Tel Source Number and the Presentation is set to Restricted (1). For example: When the following is received 'from: 100 <sip:200@201.202.203.204>', the outgoing Source Number and Display Name are set to '100' and the Presentation is set to Allowed (0). When the following is received 'from: <sip:100@101.102.103.104>', the outgoing Source Number is set to '100' and the Presentation is set to Restricted (1).

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

***ini* File [Web Interface] Parameter Name**	**Description**
MeteringType [Metering Tones Type]	Defines the metering tone (12 kHz or 16 kHz) that is detected by FXO gateways and generated by FXS gateways. 0 = 12 kHz metering tone (default). 1 = 16 kHz metering tone. **Note:** Suitable (12 kHz or 16 KHz) *coeff* must be used for both FXS and FXO gateways.
PayPhoneMeteringMode [Generate Metering Tones]	Determines the method used to configure the metering tones that are generated to the Tel side (FXS gateways only). 0 (disabled) = Metering tones aren't generated (default). 1 (internal table) = Metering tones are generated according to the internal table configured by the parameter ChargeCode. 2 (RADIUS) = N/A. **Note:** This parameter is not applicable to the Metering Tones Relay mechanism.
ChargeCode [Charge Codes Table]	The charge code table is used to configure the metering tones (and their time interval) that the FXS gateway generates to the Tel side. Up to 25 different metering rules can be defined (by repeating the parameter 25 times). To associate a metering rule to an outgoing Tel to IP call, use the Tel to IP Routing table (Prefix). ChargeCode_<Charge Code ID> = <1st period end time>,<1st period pulse interval>,<1st period pulses on answer>, <2nd period end time>,<2nd period pulse interval>,<2nd period pulses on answer>, <3rd period end time>,<3rd period pulse interval>,<3rd period pulses on answer>, <4th period end time>,<4th period pulse interval>,<4th period pulses on answer> Each Charge Code can include from a single and up to four different time periods in a day (24 hours). Each time period is composed of: - The end (in a 24-hours format) of the time period. - The time interval between pulses (in seconds). - The number of pulses sent on answer. The first time period always starts at midnight (00). It is mandatory that the last time period of each Charge Code ends at midnight (00). This prevents undefined time frames in a day. When a new call is established, the Tel to IP Routing table is searched for the destination IP address. Once a route is found, the Charge Code (configured for that route) is used to associate the route with an entry in the Charge Codes table. The gateway selects the time period by comparing the gateway's current time to the end time of each time period of the selected Charge Code. The gateway generates the Number Of Pulses on Answer once the call is connected and from that point on, it generates a pulse each Pulse Interval. If a call starts at a certain time period and crosses to the next, the information of the next time period is used. For example: ChargeCode_1 = 07,30,1,14,20,2,20,15,1,00,60,1 ChargeCode_2 = 05,60,1,14,20,1,00,60,1 ChargeCode_3 = 00,60,1
Prefix [Tel to IP Routing Table]	Prefix = <Destination Phone Prefix>, <IP Address>,<Src Phone Prefix>,<IP Profile ID>,<Charge Code> Selection of IP address (for Tel To IP calls) is according to destination and source prefixes. **Note 1:** An optional IP ProfileID (1 to 9) can be applied to each routing rule. **Note 2:** An optional Charge Code (1 to 25) can be applied to each routing rule to associate it with an entry in the ChargeCode table.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

<table>
<tr><th>ini File [Web Interface] Parameter Name</th><th>Description</th></tr>
<tr><td>EnableMediaSecurity
[Enable Media Security]</td><td>Enables or disables the Secure Real-Time Transport Protocol (SRTP).
0 = SRTP is disabled (default).
1 = SRTP is enabled.
Note: Use of SRTP reduces the number of available channels.
MP-124 18 available channels
MP-118 6 available channels
MP-114 3 available channels
MP-112 no reduction.
SRTP isn't supported on the Mediant 1000.</td></tr>
<tr><td>MediaSecurityBehaviour
[Media Security Behavior]</td><td>Determines the gateway's mode of operation when SRTP is used (EnableMediaSecurity = 1).
0 (Prefer) = The gateway initiates encrypted calls. If negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted.
1 (Must) = The gateway initiates encrypted calls. If negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected (default).</td></tr>
<tr><td>CoderName</td><td>Defines the gateway's coder list (up to five coders can be configured).
Enter coders in the following format:
CoderName=<Coder Name>,<Ptime>,<Rate>,<Payload Type>,<Silence Suppression Mode>.
<table>
<tr><th>Coder Name</th><th>Packetization Time</th><th>Rate</th><th>Payload Type</th><th>Silence Suppression</th></tr>
<tr><td>G.711 A-law [g711Alaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 8</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.711 μ-law [g711Ulaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 0</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.729 [g729]</td><td>10, 20 (default), 30, 40, 50, 60</td><td>Always 8</td><td>Always 18</td><td>Disable [0]
Enable [1]
Enable w/o Adaptations [2]</td></tr>
<tr><td>G.723.1 [g7231]</td><td>30 (default), 60, 90</td><td>5.3 [0], 6.3 [1] (default)</td><td>Always 4</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.726 [g726]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 32</td><td>Always 2</td><td>Disable [0]
Enable [1]</td></tr>
</table>
</td></tr>
</table>

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

<table>
<tr><th>ini File [Web Interface] Parameter Name</th><th>Description</th></tr>
<tr><td></td><td>Note 1: The coder name is case-sensitive.
Note 2: If silence suppression is not defined (for a specific coder), the value defined by the parameter EnableSilenceCompression is used.
Note 3: The value of several fields is hard-coded according to well-known standards (e.g., the payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored.
Note 4: Only the ptime of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined.
Note 5: If the coder G.729 is selected and silence suppression is disabled (for this coder), the gateway includes the string ‘annexb=no’ in the SDP of the relevant SIP messages. If silence suppression is enabled or set to ‘Enable w/o Adaptations’, ‘annexb=yes’ is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCEMode).

For example:
CoderName = g711Alaw64k,20,,,0
CoderName = g711Ulaw64k,40
CoderName = g7231,90,1,,1
CoderName = g726,$$,$$,,0</td></tr>
<tr><td>CoderName_ID</td><td>Defines groups of coders that can be associated with IP or Tel profiles (up to five coders in each group).
Enter coder groups in the following format:
CoderName_<coder group ID from 1 to 4>=<Coder Name>,<Ptime>,<Rate>,<Payload Type>,<Silence Suppression Mode>.
<table>
<tr><th>Coder Name</th><th>Packetization Time</th><th>Rate</th><th>Payload Type</th><th>Silence Suppression</th></tr>
<tr><td>G.711 A-law [g711Alaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 8</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.711 μ-law [g711Ulaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 0</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.729 [g729]</td><td>10, 20 (default), 30, 40, 50, 60</td><td>Always 8</td><td>Always 18</td><td>Disable [0]
Enable [1]
Enable w/o Adaptations [2]</td></tr>
<tr><td>G.723.1 [g7231]</td><td>30 (default), 60, 90</td><td>5.3 [0], 6.3 [1] (default)</td><td>Always 4</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.726 [g726]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 32</td><td>Always 2</td><td>Disable [0]
Enable [1]</td></tr>
</table>
</td></tr>
</table>

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

ini File [Web Interface] Parameter Name	Description
	Note 1: The coder name is case-sensitive. **Note 2:** If silence suppression is not defined (for a specific coder), the value defined by the parameter EnableSilenceCompression is used. **Note 3:** The value of several fields is hard-coded according to well-known standards (e.g., the payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored. **Note 4:** Only the ptime of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined. **Note 5:** If the coder G.729 is selected and silence suppression is enabled (for this coder), the gateway includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCEMode). **Note 6:** This parameter (CoderName_ID) can appear up to 20 times (five coders in four coder groups). For example: CoderName_1 = g711Alaw64k,20,,,0 CoderName_1 = g711Ulaw64k,40 CoderName_1 = g7231,90,1,,1 CoderName_2 = g726,$$,2,,0
DisconnectOnDialTone [Disconnect on Dial Tone]	FXO gateways can disconnect a call after a dial tone from the PBX is detected. 0 = Call isn't released. 1 = Call is released if dial tone is detected on the gateway's FXO port (default). **Note:** This option is in addition to the mechanism that disconnects a call when either busy or reorder tones are detected.
AAAIndications [AAA Indications]	Determines the Authentication, Authorization and Accounting (AAA) indications that are used. 0 = No indications (default). 3 = Accounting only.
RADIUSAccServerIP [RADIUS Accounting Server IP Address]	IP address of accounting server.
RADIUSAccPort [RADIUS Accounting Port]	Port number of RADIUS accounting server. The default value is 1646.
RADIUSAccountingType [RADIUS Accounting Type]	Determines when a RADIUS accounting report is issued. 0 = At the release of the call only (default). 1 = At the connect and release of the call. 2 = At the setup and release of the call.
SIPSubject [Subject]	Defines the value of the Subject header in outgoing INVITE messages. If not specified, the Subject header isn't included (default). The maximum length of the subject is limited to 50 characters.
GuardTimeBetweenCalls [Guard Time Between Calls]	Defines the time interval (in seconds) after a call has ended and a new call can be accepted for IP to Tel calls. Applicable only to FXO gateways. The valid range is 0 to 10. The default value is 1 second. **Note:** Occasionally, after a call is ended and onhook is applied, a delay is required before placing a new call (and performing offhook). This is necessary to prevent wrong hook-flash detection or other glare phenomena.
EnableUserInfoUsage [Enable User-Information Usage]	Enables or disables usage of the User Information loaded to the gateway via the User Information auxiliary file. 0 = Disable (default). 1 = Enable.
UserInfoFileName	The name (and path) of the file containing the User Information data.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

***ini* File [Web Interface] Parameter Name**	**Description**
UserInfoFileURL	Specifies the name of the User Information file and the location of the server (IP address or FQDN) from which it is loaded. http://server_name/file, https://server_name/file.
TxDTMFOption [1st to 5th Tx DTMF Option]	Determines a single or several preferred transmit DTMF negotiation methods. 0 (Not Supported) = No negotiation, DTMF digits are sent according to the parameters 'DTMFTransportType' and 'RFC2833PayloadType' (default). 3 (INFO Cisco) = Sends DTMF digits according with Cisco format. 4 (RFC 2833). 5 (INFO Nortel) = Sends DTMF digits according with IETF <draft-choudhuri-sip-info-digit-00>. 6 (NOTIFY) = Sends DTMF digits according with <draft-mahy-sipping-signaled-digits-01>. **Note 1:** DTMF negotiation methods are prioritized according to the order of their appearance. **Note 2:** When out-of-band DTMF transfer is used (3, 5 or 6), the parameter 'DTMFTransportType' is automatically set to 0 (DTMF digits are erased from the RTP stream). **Note 3:** When RFC 2833 (2) is selected, the gateway: Negotiates RFC 2833 Payload Type (PT) using local and remote SDPs. Sends DTMF packets using RFC 2833 PT according to the PT in the received SDP. Expects to receive RFC 2833 packets with the same PT as configured by the parameter 'RFC2833PayloadType'. Uses the same PT for send and receive if the remote party doesn't include the RFC 2833 DTMF PT in its SDP. **Note 4:** When TxDTMFOption is set to 0, the RFC 2833 PT is set according to the parameter 'RFC2833PayloadType' for both transmit and receive. ***ini* file note:** The DTMF transmit methods are defined using a repetition of the same (TxDTMFOption) parameter (up to five options can be provided).
DelayBeforeDIDWink [Delay Before DID Wink]	Defines the time interval (in seconds) between detection of offhook and generation of DID Wink. Applicable only to FXS gateways. The valid range is 0 to 1,000. The default value is 0.
Send180ForCallWaiting	0 = Use 182 Queued response to indicate a call waiting (default). 1 = Use 180 Ringing response to indicate a call waiting.
3xxBehavior	Determines the gateway's behavior when a 3xx response is received for an outgoing INVITE request. The gateway can either use the same call identifiers (CallID, branch, to and from tags) or change them in the new initiated INVITE. 0 (forward) = Use different call identifiers for a redirected INVITE message (default). 1 (redirect) = Use the same call identifiers.
NumberOfActiveDialogs	Defines the maximum number of active SIP dialogs that are not call related (i.e., REGISTER and SUBSCRIBE). This parameter is used to control the Registration / Subscription rate. The valid range is 1 to 5. The default value is 5.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

ini File [Web Interface] Parameter Name	Description
WaitForDialTime [Wait For Dial Time]	Determines the delay before the gateway starts dialing on the FXO line in the following scenarios (applicable only to FXO gateways): 1. The delay between the time the line is seized and dialing is begun, during the establishment of an IP→Tel call. **Note:** Applicable only to FXO gateways for single stage dialing, when waiting for dial tone (IsWaitForDialTone) is disabled. 2. The delay between the time when Wink is detected and dialing is begun, during the establishment of an IP→Tel call (for DID lines, EnableDIDWink = 1). 3. For call transfer. The delay after hook-flash is generated and dialing is begun. The valid range (in milliseconds) is 0 to 20000 (20 seconds). The default value is 1000 (1 second).
FXSOOSBehavior [Out-Of-Service Behavior]	Determines the behavior of FXS endpoints that are not defined (in the Endpoint Phone Number table), and the behavior of all FXS endpoints when a Busy-Out condition exists. 0 (None) = Normal operation: No response is provided to undefined endpoints. Dial tone is played to FXS endpoints when a Busy-Out condition exists. 1 (Reorder Tone) = The gateway plays a reorder tone to the connected phone/PBX (default). 2 (Polarity Reversal) = The gateways reverses the polarity of the endpoint, marking it as unusable (relevant, for example, to PBX DID lines).This option can't be configured on-the-fly. 3 (Polarity Reversal + Reorder Tone) = Same as 2 and 3 combined. This option can't be configured on-the-fly.
CountryCoefficients	Determines the FXO line characteristics (AC and DC) according to country of origin. Argentina = 0, Australia = 1, Austria = 2, Bahrain = 3, Belgium = 4, Brazil = 5, Bulgaria = 6, Canada = 7, Chile = 8, China = 9, Colombia = 10, Croatia = 11, Cyprus = 12, Czech_Republic = 13, Denmark = 14, Ecuador = 15, Egypt = 16, El_Salvador = 17, Finland = 18, France = 19, Germany = 20, Greece = 21, Guam = 22, Hong_Kong = 23, Hungary = 24, Iceland = 25, India = 26, Indonesia = 27, Ireland = 28, Israel = 29, Italy = 30, Japan = 31, Jordan = 32, Kazakhstan = 33, Kuwait = 34, Latvia = 35, Lebanon = 36, Luxembourg = 37, Macao = 38, Malaysia = 39, Malta = 40, Mexico = 41, Morocco = 42, Netherlands = 43, New_Zealand = 44, Nigeria = 45, Norway = 46, Oman = 47, Pakistan = 48, Peru = 49, Philippines = 50, Poland = 51, Portugal = 52, Romania = 53, Russia = 54, Saudi_Arabia = 55, Singapore = 56, Slovakia = 57, Slovenia = 58, South_Africa = 59, South_Korea = 60, Spain = 61, Sweden = 62, Switzerland = 63, Syria = 64, Taiwan = 65, TBR21 = 66, Thailand = 67, UAE = 68, United_Kingdom = 69, UnitedStates = 70, Yemen = 71 The default value is 70 (United States).
TelConnectCode [Send Digit Pattern on Connect]	Defines a digit pattern that is sent to the Tel side after 200 OK is received from the IP side. The digit pattern is a predefined DTMF sequence that is used to indicate an answer signal (e.g., for billing purposes). Applicable only to FXS gateways. The valid range is 1 to 8 characters.
VoiceMenuPassword [Voice Menu Password]	Password for the voice menu, used for configuration and status. To activate the menu, connect an analog telephone and dial *** (three stars) followed by the password. The default value is 12345.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

***ini* File [Web Interface] Parameter Name**	**Description**
ActivityListToLog [Activity Types to Report via 'Activity Log' Messages]	The Activity Log mechanism enables the gateway to send log messages (to a Syslog server) that report certain types of web actions according to a pre-defined filter. The following filters are available: **PVC** (Parameters Value Change) - Changes made on-the-fly to parameters. **AFL** (Auxiliary Files Loading) - Loading of auxiliary files (e.g., via Certificate screen). **DR** (Device Reset) - Device reset via the Reset Device screen. **FB** (Flash Memory Burning) - Burning of files / parameters to flash (e.g., Save Configuration screen). **SWU** (Device Software Update) - cmp loading via the Software Upgrade Wizard. **ARD** (Access to Restricted Domains) - Access to Restricted Domains. The following screens are restricted: (1) ini parameters (AdminPage) (2) General Security Settings (3) Configuration File (4) IPSec/IKE tables (5) Software Upgrade Key (6) Internal Firewall (7) Web Access List. (8) Web User Accounts **NAA** (Non Authorized Access) - Attempt to access the Embedded Web Server with a false / empty username or password. **SPC** (Sensitive Parameters Value Change) - Changes made to sensitive parameters: (1) IP Address (2) Subnet Mask (3) Default Gateway IP Address (4) ActivityListToLog For example: ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'
Internal Firewall Parameters	
AccessList_Source_IP [Source IP]	IP address (or DNS name) of source network, or a specific host.
AccessList_Net_Mask [Mask]	IP network mask. 255.255.255.255 for a single host or the appropriate value for the source IP addresses. The IP address of the sender of the incoming packet is bitwise ANDed with this mask and then compared to the field 'Source IP'.
AccessList_Start_Port **AccessList_End_Port** [Local Port Range]	The destination UDP/TCP ports (on this device) to which packets are sent. The valid range is 0 to 65535. **Note:** When the protocol type isn't TCP or UDP, the entire range must be provided.
AccessList_Protocol [Protocol]	The protocol type (e.g., UDP, TCP, ICMP, ESP or 'Any'), or the IANA protocol number (in the range of 0 (Any) to 255). **Note:** The protocol field also accepts the abbreviated strings 'SIP', 'MGCP', 'MEGACO' and 'HTTP'. Specifying these strings implies selection of the TCP or UDP protocols, and the appropriate port numbers as defined on the device.
AccessList_Packet_Size [Packet Size]	Maximum allowed packet size. The valid range is 0 to 65535. **Note:** When filtering fragmented IP packets, the Packet Size field relates to the overall (reassembled) packet size, not to the size of each fragment.
AccessList_Byte_Rate [Byte Rate]	Expected traffic rate (bytes per second).
AccessList_Byte_Burst [Burst Bytes]	Tolerance of traffic rate limit (number of bytes)

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

***ini* File [Web Interface] Parameter Name**	**Description**
AccessList_Allow_Type [Action Upon Match]	Action upon match (allow or block)
AccessList_MatchCount [Match Count]	A read-only field that provides the number of packets accepted / rejected by a specific rule.
PPPoE Parameters	
EnablePPPoE	Enables the PPPoE (Point-to-Point Protocol over Ethernet) feature. 0 = Disable (default) 1 = Enable
PPPoEPassword	Password for PAP or Secret for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0.
PPPoERecoverIPAddress	IP address to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 10.4.10.4.
PPPoERecoverDfgwAddress	Default GW address to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 10.4.10.1.
PPPoERecoverSubnetMask	Subnet Mask to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 255.255.0.0.
PPPoEServerName	Server Name for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0.
PPPoEStaticIPAddress	IP address to use in a static configuration setup. If set, used during PPP negotiation to request this specific IP address from the PPP server. If approved by the server, this IP address is used during the session. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 0.0.0.0.
PPPoEUserName	User Name for PAP or Host Name for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0.
Differential Services Parameters	
NetworkServiceClassDiffServ [Network QoS]	Sets the DiffServ value for Network service class content. The valid range is 0 to 56. The default value is 48.
PremiumServiceClassMediaDiffServ [Media Premium QoS]	Sets the DiffServ value for Premium Media service class content (only if IPDiffServ is not set in the selected IP Profile). The valid range is 0 to 56. The default value is 46. **Note:** The value for the Premium Control DiffServ is determined by (according to priority): (1) IPDiffServ value in the selected IP Profile. (2) PremiumServiceClassMediaDiffServ.
PremiumServiceClassControlDiffServ [Control Premium QoS]	Sets the DiffServ value for Premium Control service class content (only if ControlIPDiffserv is not set in the selected IP Profile). The valid range is 0 to 56. The default value is 46. **Note:** The value for the Premium Control DiffServ is determined by (according to priority): (1) ControlPDiffserv value in the selected IP Profile. (2) PremiumServiceClassControlDiffServ.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 59 to 70)

***ini* File [Web Interface] Parameter Name**	**Description**
GoldServiceClassDiffServ Gold QoS	Sets the DiffServ value for the Gold service class content. The valid range is 0 to 56. The default value is 26.
BronzeServiceClassDiffServ [Bronze QoS]	Sets the DiffServ value for the Bronze service class content. The valid range is 0 to 56. The default value is 10.

4.7 Version History

Details of previous releases can be found in the Release Notes of Version 4.6, published by AudioCodes on Jul-13-2005.

Reader's Notes

AudioCodes™ Analog Media Gateways & CPE

SIP

MediaPack™ MP-124 & MP-11x

Release Notes Version 5.0

AudioCodes

www.audiocodes.com